
Nortel Secure Networks

Entrust/Client

User Guide

for UNIX

Publication number: 68009.08

Date: August 1996

Software release: 2

© 1994–1996 Northern Telecom Limited

All rights reserved.

Printed in Canada

This information is subject to change as Northern Telecom Limited reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

Nortel, Entrust, Entrust/Client, Entrust/Manager, Entrust/Officer, and Entrust/Admin are trademarks of Northern Telecom Limited. IBM is a trademark of International Business Machines. Microsoft, Windows, Windows 95, and Windows NT are trademarks of Microsoft Corporation. UNIX is a trademark of X/Open Company Ltd. Macintosh is a trademark of Apple Computer, Inc. RSA is under license from Public Key Partners, Inc. HP is a trademark of Hewlett-Packard Company. SunOS and Solaris are trademarks of Sun Microsystems Inc. X Windows is a trademark of Massachusetts Institute of Technology.

Entrust/Client User Guide

Contents

About this guide 1

Purpose of this user guide 1

What you need to know 1

Terminology 2

Notational conventions 3

About Entrust/Client 5

Reasons for using Entrust/Client 8

Protecting your work 8

Signing documents electronically 10

Sample uses of Entrust/Client 10

Encrypting a contract bid for a customer 10

Encrypting employee yearly performance evaluations 11

Encrypting an electronic mail message 11

Signing a form 12

What Entrust/Client is not 13

Before you begin 15

Minimum system requirements 15

Start-up package 16

Important information about passwords 17

Getting help 18

Installing Entrust/Client 19

Installation procedure 20

Post-installation tasks 21

Getting started with Entrust/Client	23
Setting up the Client	23
Starting Entrust/Client for the first time	26
Encrypting and signing your first files	31
Decrypting and verifying your first protected files	42
Ending your Entrust/Client session	45
Using Entrust/Client	47
Protecting the contents of your files	48
Selecting files to encrypt and sign	48
Selecting recipients for your encrypted files	51
Selecting encrypting and signing options	66
Encrypting and signing files	70
Deleting files so that they are unrecoverable	73
Decrypting and verifying protected files	76
Exchanging protected files with users in different domains	83
Creating and accessing your address book	84
Building your address book	86
Changing the contents of your address book	89
Exporting your personal Entrust address	91
Using saved lists of recipients	93
Accessing recipient list management functions	94
Creating a new recipient list	95
Changing an existing recipient list	98
Deleting an existing recipient list	100
Sharing recipient lists	101
Changing your Entrust/Client password	106
Creating additional Entrust/Client usernames	108
Recovering your Entrust/Client username	112
Setting options for Entrust/Client	116
Using Entrust/Client on different computers	119
Starting Entrust/Client	120
Logging on to Entrust/Client	121
Logging off from Entrust/Client	124
Ending your Entrust/Client session	124

Hints	125
Forgotten password or lost or damaged Client profile	125
Using Entrust/Client in different time zones	125
Intended recipient cannot decrypt my files	126
Cannot update your Entrust signature verification information	127
Search information is unavailable	128
Logging on to the Client after your personal Entrust information has been changed	129
Logging on to the Client after your name has been changed	129
Importing a key certified by a CA with the same name as your CA	130
Appendix A: Entrust/Client shortcuts	131
Appendix B: Entrust/Client user files	133
Appendix C: Entrust password security	137
Appendix D: Entrust specifications	141
List of terms	145
Index	149

About this guide

Purpose of this user guide

This guide

- describes general cryptography concepts
- details the Entrust/Client installation procedure
- gives step-by-step instructions on how to use Entrust/Client

The “Getting started with Entrust/Client” chapter starting on page 23 is a detailed tutorial that takes you through the processes of creating your Entrust/Client username, encrypting and signing your first files, and finally decrypting and verifying the files you encrypted and signed.

The chapter titled “Using Entrust/Client” on page 47 explains how to use all Entrust/Client functions.

What you need to know

This user guide is intended for people who have some experience with UNIX. Users should be familiar with terms and commands such as the following:

- path
- directory
- shell
- cd
- ls
- executable

For information about these terms, refer to your UNIX documentation.

Terminology

Table 1 shows terms that are equivalent and gives a brief description of each. The short terms are used most often to improve the readability of this guide.

Table 1: Terms used in this guide

Term	Short version	Description
Entrust/Client	Client	a software application
Entrust/Client user	user	a person who uses the Client
Entrust Administrator	Administrator	the person who is responsible for the day-to-day activities involved in the administration of users
UNIX System Administrator	System Administrator	the person who is typically responsible for installing the Client software
Certification Authority	CA	refers collectively to the people who are responsible for setting security policies and assigning secure electronic identities in the form of certificates
CA security domain	domain	group of people who use Entrust under the same software license and have been certified by the same CA

The term *Entrust* used alone refers to Entrust products in general.

The expression *protected files* refers to files that have been encrypted, signed, or both encrypted and signed. Encrypted (but not signed) files have been processed by the Client in such a way that they can only be read by authorized people.

Digital signatures on signed (but not encrypted) files can be verified by any Entrust/Client user, but a warning will appear if the files have been tampered with after they were signed. Therefore, encryption and digital signatures protect data in different ways.

Notational conventions

Commands that must be entered at a UNIX prompt are preceded by the % symbol which represents the UNIX prompt; for example,

% ls -lrt

The following types of information appear in italics:

- filenames and paths
- titles of documents
- window and dialog names
- names of items that appear in windows and dialogs
- terms that require emphasis

About Entrust/Client

Entrust/Client is an application that lets you encrypt and attach your digital signature to any file. You can also decrypt files and verify the signature on a file that was encrypted and signed using the Client.

The Client provides security features such as:

- data privacy
- signature authentication
- data integrity
- automated key management

Data privacy means only you and people you authorize (these people are called recipients) can view the contents of the files you encrypt.

Signature authentication means that you can verify the digital signature of the person who signed a file. Data integrity means the file has not been altered since it was signed. The digital signature that accompanies a file is a guarantee that the file was signed by the author and that the file has not been altered since it was signed.

Automated key management means it is easy for you to protect and unprotect files. The Entrust software keeps track of each Client user so you do not have to.

Table 2 on page 6 summarizes the main Entrust/Client features.

Table 2: Main Entrust/Client features

Feature	Description
privacy	You have assurance that only you and authorized recipients can look at the contents of files you encrypt.
authentication	This feature allows you to verify the identity of the person who signed a file.
integrity	When you verify a signed file, this feature warns you if a file has been altered since it was signed.
portability	If you need to use Entrust/Client on a different computer than the one you normally use, you only need to transfer a copy of a file called your Client profile to the computer you want to use (provided the Client is installed on that computer). You can do this using a floppy diskette or any other file transfer mechanism. Your profile is portable across Macintosh computers, UNIX workstations, and PCs running Microsoft Windows. For more information, see "Using Entrust/Client on different computers" on page 119.
address book services	This feature allows you to exchange protected files with a person who uses the Client in a different CA security domain. For more information, see "Exchanging protected files with users in different domains" on page 83.
recipient lists	A recipient list is a set of options and recipients that you select and store under a recipient list name. Instead of having to specify each recipient and option every time you want to encrypt a file, you can specify the name of a recipient list. You control who is part of a recipient list and you can create more than one recipient list. For example, you could create one recipient list for each project you work on. For more information, see "Using saved lists of recipients" on page 93.
shared recipient lists	It is possible to share recipient lists with other Client users. Shared recipient lists let you maintain single copies of recipient lists and store them in a directory that is accessible to everyone who needs them. You can share your own recipient lists by exporting them. You can share other users' exported recipient lists by importing them.
—continued—	

Table 2: Main Entrust/Client features (continued)

Feature	Description
file compression	You can compress protected files to save disk space. When compressed and protected files are received at the intended destination, they are automatically decompressed.
file archiving	You can use the <i>Archive</i> option to store multiple protected files in a single archive file. This is useful if you want to transfer several protected files; by storing all the protected files in a single archive file, you only need to transfer a single file. When the file is received at the intended destination and decrypted, the files are restored with their original filenames.
secure file deletion	You can use the secure delete function to perform a true deletion of files. A true delete means that files deleted with this function are completely unrecoverable using any file-recovery utility.
search bases	Your Security Officer can provide you with one or more search bases that you can use to reduce the scope of your recipient searches and thereby speed up the process of selecting recipients.
ASCII file format support	This feature lets you encode files in a manner that ensures data integrity when you transfer files from one computer to another using a file transfer mechanism designed for ASCII transfer only.

Reasons for using Entrust/Client

Protecting your work

Anyone who has access to your files, whether they are stored on floppy diskettes, hard disks, or a shared file server, can also see the contents of the files. In general, you may not mind if your colleagues can see the contents of your files; however, you probably have files that are sensitive and should only be seen by you and other people with whom you choose to share them. You can protect your sensitive files by using the Client to encrypt and sign them.

An encrypted file is completely unreadable. That means no one, including you, can read an encrypted file until it is decrypted. To decrypt an encrypted file is to restore it to its original state. Only you and other authorized recipients can decrypt the protected file and only you can determine who those recipients will be.

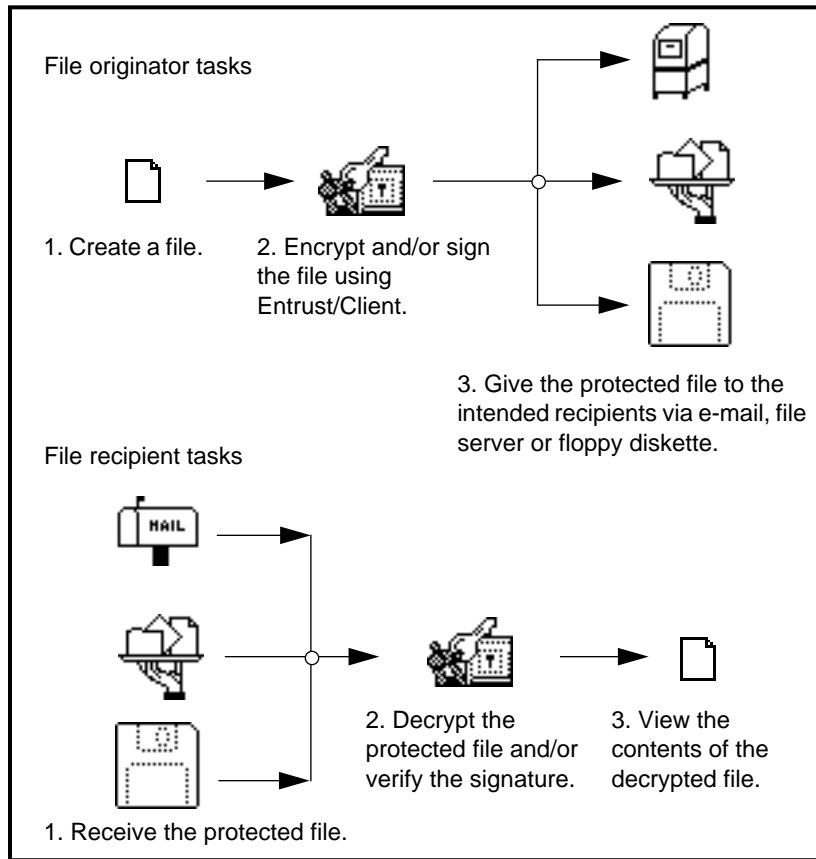
ATTENTION

Entrust/Client does not prevent anyone from getting copies of your files. The Client makes it infeasible for unauthorized people to view the original contents of the files.

Once the file is protected, you can give a copy to your intended recipients to decrypt and read when convenient.

There are no restrictions on how you combine recipients and encrypted files. For example, you can encrypt files for one group of people and then encrypt some other files for other groups or individuals. The Client keeps track of who is authorized to decrypt each individual file.

Entrust/Client is part of a suite of tools you use in your day-to-day activities. Note that using the Client is optional and is only necessary when you want to encrypt and sign a file. Figure 1 on page 9 summarizes the encryption and signing process, and the decryption and verification process.

Figure 1 Where Entrust/Client fits in your day-to-day activities

Since the file can only be decrypted by you and the recipients, it does not matter how you give the file to the recipients. You can put the file in a directory to which your recipients have access, transfer the file using any electronic file transfer tool, or you can attach the protected file to an electronic mail message which you send to the recipients.

Note: Protected files are generally created in binary format. If you send protected files using an electronic file transfer tool, or as e-mail attachments, ensure these tools can handle binary files. If not, you can use the *ASCII encode after encrypting* option when you protect files that are to be sent using tools or network services that only handle ASCII files.

Signing documents electronically

You can use Entrust/Client to place your personal digital signature on a file whether or not the file is also encrypted. This signature is a guarantee that the file came from you and that it has not been altered since it was signed.

A digital signature offers a certain level of protection even if a file is not encrypted because it is a guarantee that no one has tampered with the file. The Client is used to verify the signature on signed files. If the signature is valid, it means that the file has not been tampered with since the time it was signed. But if the signature verification fails, it means that the file may have been tampered with and that a new copy of the signed file should be obtained from the person who signed the file.

Sample uses of Entrust/Client

The following scenarios give examples of how people often use the Client in their day-to-day activities. Two fictional characters, named Bob and Alice, are used to describe the scenarios.

Encrypting a contract bid for a customer

Bob finally finished the sensitive contract bid he has been working on day and night for two weeks, and he needs to send it to his customer, Alice. Bob planned to use the mail to send the bid stored on a floppy diskette, but he worried that the diskette might fall into the wrong hands. Bob's bid must be protected from being read by anyone else. Since Alice also uses Entrust, Bob can easily protect his bid so that only she can retrieve the information. In addition, he can include his digital signature with the encrypted file to provide Alice with the added peace of mind that no one has tampered with his bid.

Before Bob sends the bid to Alice, he follows the procedure shown below.

1. Start the Client.
2. Specify the name of the recipient for this bid—in this case, Alice.
3. Encrypt and digitally sign a copy of the file containing the bid.
4. Copy the encrypted and signed file to a floppy diskette.

Now that Bob's bid is protected, he can simply put the floppy diskette in the mail, knowing that only Alice can read the contents. Even if the diskette falls into the wrong hands, he can be certain that its contents will not be revealed. Bob's file is protected by Entrust.

Encrypting employee yearly performance evaluations

Alice is preparing yearly performance review reports for her employees and wants to make the reports available to the other managers in her division. While Alice wants it to be easy for those managers to read the reports, she must ensure that the information remains confidential (employees must not have access to each other's reports). The easiest way for Alice to make the reports available to the other managers is to store copies of the reports on a shared file server in her network. But since everyone in the company has access to this file server, she must ensure that only the managers can read the reports.

Before Alice stores copies of her employees' yearly performance review reports on the file server, she follows the procedure shown below.

1. Start the Client.
2. Specify the names of the recipients for the reports—in this case, the other managers in Alice's division.
3. Encrypt and digitally sign copies of each file containing an employee's performance review.
4. Copy the encrypted and signed files to a directory on the file server.
5. Notify the managers that the files are available and that they must be unprotected before they can be read.

Encrypting an electronic mail message

Bob is working on a proposal for a new product that is likely to be a great commercial success, and he wants a colleague's opinion on his work so far. The only problem is that Bob's colleague, Alice, works in another city. Bob could fax a copy of his proposal, but he hesitates since it is critical that the proposal remain secret until it is ready to be unveiled. Bob decides to send the proposal to Alice as an attachment to an electronic message.

In general, sending a file attached to an electronic mail message makes the contents of the file accessible to anyone who can read copies of other people's electronic mail as it is transmitted over the network. The technology for this type of illegal activity is readily available.

Because of the highly sensitive nature of the proposal and the great potential for disaster if it were to fall into the wrong hands, Bob decides to protect it from being read by anyone else. Since Alice also uses Entrust, he can use the Client to protect the proposal.

To protect a copy of the proposal before sending it, Bob follows the procedure shown below.

1. Start the Client.

2. Specify the name of the recipient for the proposal—in this case, Alice.
3. Encrypt and digitally sign a copy of the file containing the proposal.
4. Switch to an electronic mail tool.
5. Compose an electronic mail message to Alice (in this case) asking for opinions on the proposal.
6. Attach the encrypted and signed proposal to the mail message.

Bob can now safely send the proposal.

Alice detaches the file containing the proposal, decrypts it, annotates the proposal with comments, re-encrypts it, and returns it to Bob using electronic mail.

No one except Bob and Alice can ever know the contents of the proposal until Bob decides to make the information available.

Signing a form

In an effort to move towards a paperless office, Alice's company has online versions of its business forms (for example, expense reports). Alice routinely completes such forms directly online using her computer. Then she has to print the form for her supervisor Bob to sign.

Instead of printing the form for signature, Alice can use the Client to digitally sign the form and send it electronically to Bob for authorization. Bob checks the form, authorizes it by digitally signing it (without printing it to paper), and sends it directly to Accounting. Because the form does not contain sensitive information, it does not need to be encrypted.

Since Accounting also uses Entrust, the signature on the form can be verified to ensure that the form was authorized by Bob and that it has not been altered by anyone.

Alice would first follow the procedure shown below.

1. Open the file containing the form and fill it out online.
2. Save the changes in a file.
3. Use the Client to sign the file.
4. Use the file transfer mechanism of choice to send the file to Bob.

Bob would then follow the procedure shown below.

1. Start the Client.
2. Verify the form.
3. Use the Client to sign the file.

4. Use a file transfer mechanism to forward the file to Accounting.

Accounting would then follow the procedure shown below.

1. Start the Client.
2. Use the Client to verify Bob's signature and the integrity of the contents of the file.

What Entrust/Client is not

The Client is neither a substitute for your existing electronic mail software nor is it a substitute for an electronic file transfer mechanism. Once you have protected a file using the Client, you must use an existing tool to send the protected file to your recipient. An Entrust recipient should not be considered equivalent to an electronic mail recipient.

Before you begin

Before you begin to install and use Entrust/Client

- Ensure the computer you plan to use with the Client meets the minimum requirements specified in “Minimum system requirements” on this page.
- Obtain your start-up package from your Administrator (refer to “Start-up package” on page 16).
- Read “Important information about passwords” on page 17.

Minimum system requirements

The Client runs on HP and Sun workstations. The following operating systems are supported:

- HP-UX 9.03 or HP-UX 9.05
- HP-UX 10
- SunOS 4.1.3 and 4.1.4
- Solaris 2.4

You also need an X11R5 or better X server and a window manager.

Note: It is recommended that you use the OSF/Motif Window Manager.

If you are unsure of whether or not your system meets these requirements, contact your UNIX System Administrator.

Start-up package

Before you can use the Client, you need to obtain important information and files from your Entrust Administrator. Ask your Administrator to give you the following information:

- an Entrust user reference number
- an Entrust user authorization code
- the path to the following:
 - Client *setup* script
 - Client software

Reference number and authorization code

You need a reference number (for example, 91480170) and an authorization code (for example, CMTJ-8VOR-VFNS) to create your Client username. Your Administrator will tell you your reference number and authorization code in a confidential and secure manner.

ATTENTION

Keep your reference number and authorization code confidential. Ensure you destroy them after you have created your Client username.

The reference number and authorization code can only be used once. If you need to create more than one Client username refer to “Creating additional Entrust/Client usernames” on page 108.

Access to the Client setup script

You will need to run the *setup* script to configure your Client environment. See “Setting up the Client” on page 23 for more information.

Access to the Client software

You will need to add the path to the Client executable to your execution path. See “Setting up the Client” on page 23 for more information.

Important information about passwords

Your Entrust/Client password is a critical link in the security chain. You should never reveal your password to anyone. You should guard your password just as you would a banking card personal identification number (PIN) or other valuable information.

ATTENTION

If you write down your password, ensure it is stored in a locked place that only you can access. Anyone with access to your password and your Client profile will have the ability to view your protected files and to sign files with your signature. If you forget your password or if you suspect that someone has obtained your password, contact your Entrust Administrator.

It is important that you select passwords that are difficult to guess or derive. Avoid using the following as passwords because they are easy for an intruder to obtain:

- common or proper nouns
- birth dates
- employee numbers
- social security numbers
- any number that can be associated with you

When you choose a password, invent a word and include special characters for good measure. Examples of special characters are: \$, +, !, =, ~, ^ and &. A good password is one that is difficult to guess yet easy to remember (for example, H2OPlsNow! (water please, now!)).

In addition, the software enforces certain rules that make your password difficult to obtain. Your password must

- be at least eight characters long (however, as you make your password longer, it becomes significantly more difficult for an attacker to guess the password you select)
- contain at least one upper case letter
- contain at least one lower case letter
- not contain many occurrences of the same character
- not be the same as your Entrust/Client username
- not contain a lengthy substring of your Entrust/Client username

For more information about password criteria and how Entrust manages password security, refer to “Appendix C: Entrust password security.”

Getting help

Entrust/Client comes with online help. Click the Help button on the currently displayed dialog to obtain help for that dialog.

Refer to “Hints” on page 125 to get help with some common problems. If you need additional help, contact your Entrust Administrator.

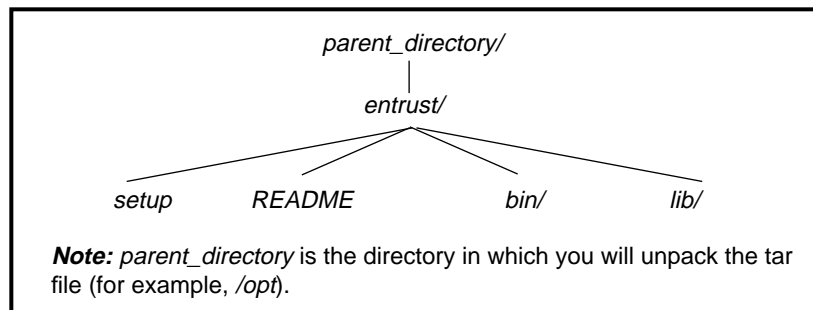
Installing Entrust/Client

While there are many approaches you may take to install the Client, this chapter explains how to install the Client software on servers on which the Client is required. Therefore, this chapter is intended for UNIX System Administrators who have the necessary privileges to install software on servers. Alternatively, any user can perform a local installation of the Client software by following the procedures in this chapter.

The Client software is shipped with the Entrust infrastructure software and is stored in the `/opt/entrust/clients` directory on the workstation on which the Entrust infrastructure software was installed. The `/opt/entrust/clients` directory contains one tar file for each supported platform. A tar file is an archive of directories and files that have been *packed* together in a single large file. A tar file is convenient for shipping software. When a tar file is *unpacked*, the original tree structure is preserved. Transfer a copy of the appropriate tar file to the server on which you want to install the Client.

Before installing the Client software, decide on an appropriate directory (for example, `/opt`). This directory is referred to as the *parent_directory* in this user guide. This is the directory in which the *entrust* directory (and its subdirectories) will be created. See Figure 2 for an example.

Figure 2 Entrust directory structure



Installation procedure

To install the Client software, simply unpack the tar file as follows:

1. % `cd parent_directory`

where *parent_directory* is the directory in which you want to unpack the tar file (for example, */opt*).

Note: If you are installing the Client on the same workstation as the one on which Entrust/Manager is installed, then the parent directory must be */opt*.

2. % `tar xvf device_name/tarfile`

where *device_name* refers to the magnetic tape device that will be used to load the magnetic tape containing the Client software (for example */dev/rst0*). The actual device filename used on your system may be quite different. The UNIX System Administrator can provide you with the device filename.

tarfile refers to the filename of the tar file you received (for example, *ENTUXCLI.TAR.SUN.DOM*).

Once the tar file is unpacked, the *entrust* directory is created within the *parent_directory* (for example, */opt*). The following files and directories are created within the *entrust* directory:

- *setup* script
- *README* file
- *bin* directory
- *lib* directory

The *setup* script must be run by each user before using the Client for the first time (see “Configuring your Client environment” on page 24). The *README* file contains the most up-to-date installation information. The *entrust/bin* directory contains the *xentrust* file. The *xentrust* file contains the Entrust/Client software. Users should add the *entrust/bin* directory to their path so they can start up the Client (see “Adding the Client software to your path” on page 25). The *lib* directory contains files required by the Client.

You should now perform the tasks described in “Post-installation tasks” on page 21.

Post-installation tasks

Once you have unpacked the tar file, copy the *entrust.ini* file to the *entrust* directory (for example, */opt/entrust*). The *entrust.ini* file was created when Entrust/Manager was installed and set up in your organization. This file contains important information required by the Client software. Without this file, it will not be possible to run the Client.

ATTENTION

If you are running Solaris 2.4, the Client software dynamically accesses the OSF/Motif runtime library. Therefore the OSF/Motif runtime library (filename is *libXm.so.3*) must exist in the */usr/dt/lib* directory. This library is included with Solaris but, for your convenience, a copy of the *libXm.so.3* file is provided in the *entrust/lib* directory with the Client software. Without the presence of the *libXm.so.3* file in the */usr/dt/lib* directory, you will not be able to run the Client. If you are running SunOS 4.1.3 or HP-UX, the OSF/Motif runtime library is statically linked; therefore, the *libXm.so.3* file is not required.

Now users can now set themselves up to run the Client. Refer to “Getting started with Entrust/Client” on page 23.

Getting started with Entrust/Client

This chapter contains the information you need to start using the Client. It provides you with step-by-step instructions for completing the following tasks:

- setting up the Client
- starting the Client
- creating a Client username
- encrypting and signing a file
- decrypting and verifying a protected file
- ending your Client session

Setting up the Client

Before you can run the Client software, you must perform the following tasks:

- Configure your Client environment.
- Add the Client software to your execution path.
- Add the OSF/Motif runtime library to your LD_LIBRARY_PATH (Solaris users only).

Note: You need to perform these tasks before running the Client. To perform these tasks, you will need the information described in “Start-up package” on page 16.

Configuring your Client environment

Configuring your Client environment involves running the *setup* script to create your *.entrustrc* file. This file is used to store the path to the directory in which the Client software is installed, and other information required by the Client. The *.entrustrc* file is created in your home directory and should not be moved. For more information about this file, refer to “Appendix B: Entrust/Client user files.”

To create your *.entrustrc* file, proceed as follows:

1. % cd *parent_directory/entrust*

where *parent_directory* is the directory in which the Client software was installed (for example, */opt/entrust*).

If you do not know the path, ask your System Administrator.

2. Enter

% *.setup*

Messages similar to the following appear on the screen.

Checking contents and suitability of current working directory.

A new ".entrustrc" has been created in your home directory.

Before running Entrust for the first time, you must ensure that the site-specific configuration file "entrust.ini" has been installed on this system as

/opt/entrust/entrust.ini

You may also want to add

/opt/entrust/bin

to your execution path.
See the README file for details.

Once these steps are complete, you are ready to run Entrust!

The next thing you should do is add the path to the Client software to your execution path.

Adding the Client software to your path

To have access to the Client software, add the path to the Client executable (*xentrust*) to your execution path as explained in this section.

If you are a C shell user, add the following command to your *.cshrc* or *.login* file:

```
setenv PATH path_to_entrust:${PATH}
or
set path = (path_to_entrust $path)
```

where *path_to_entrust* is the path to the Client executable (*xentrust*); for example, */opt/entrust/bin*.

If you are a Bourne or Korn shell user, add the following command to your *.profile*:

```
PATH=path_to_entrust:${PATH}
```

where *path_to_entrust* is the path to the Client executable (*xentrust*); for example, */opt/entrust/bin*.

Korn shell users can also add the PATH command to their *.kshrc* or \$ENV file.

You are now set up to run the Client software. You can start up the Client and create a Client username.

Adding the OSF/Motif runtime library to your LD_LIBRARY_PATH

This section only applies to Solaris users.

You should add the */usr/dt/lib* directory to your LD_LIBRARY_PATH.

If you are a C shell user, add the following command to your *.cshrc* or *.login* file:

```
setenv LD_LIBRARY_PATH /usr/dt/lib:${LD_LIBRARY_PATH}
```

Starting Entrust/Client for the first time

This procedure assumes that the following tasks have been completed:

- the Client has been installed
- you performed the tasks in “Setting up the Client” on page 23
- you obtained your start-up package from your Entrust Administrator

To start up the Client and create a username, proceed as follows:

1. Enter the following command:

```
% xentrust
```

The *Welcome to Entrust* dialog appears.



2. Click *Create User...*

The *Create New User* dialog appears. Notice the *Field description* area at the bottom of the dialog. This area provides a brief description of the information you need to enter in each field of the dialog. Simply click in any

field and the corresponding description will appear in the *Field description* area.

Create New User

User information

Username (8 char max):

Directory:

User Password:

Password Confirm:

Administrator-supplied information

Reference Number:

Authorization Code:

Field description

Enter any name up to eight characters. This name will be your Client username.

OK Cancel Help

3. Enter a name in the *Username* field.

You can choose any name you like but you are limited to eight characters; for example, *johnsmit*.

4. Tab to the *Directory* field and enter the name of the directory in which you want to store your profile (normally your home directory).

Your profile is a file that contains critical information about you that is required by Entrust. This critical information is encrypted to ensure security. For increased security, you can store this file in a directory to which only you have access. Regardless of where you store your profile, you must ensure that no one can get access to it.

The filename of your profile is the same as your username. An *epf* filename extension (for example, *johnsmit.epf*) is automatically added to the filename of the profile.

5. Tab to the *User Password* field and enter a password.

Your Client password must

- be at least eight characters long (however, as you make your password longer, it becomes significantly more difficult for an attacker to guess the password you select)

- contain at least one upper case letter
- contain at least one lower case letter
- not contain many occurrences of the same character
- not be the same as your Client username
- not contain a lengthy substring of your Client username

The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: \$, +, =, !, ~, ^ and &. A good password is one that is difficult to guess yet easy to remember (for example, H2OPIsNow! (water please, now!)). For more information about passwords, refer to "Appendix C: Entrust password security."

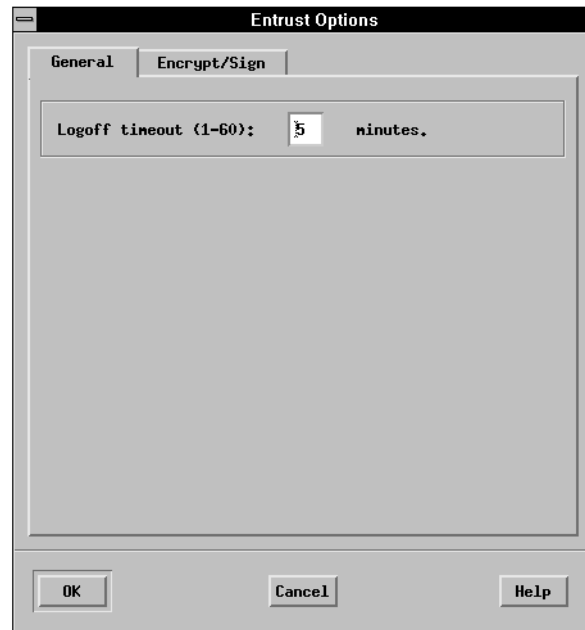
6. Tab to the *Password Confirm* field and enter the same password again.

The reason you need to enter your new password twice is to ensure that you typed exactly what you intended to type. The Client checks to ensure that you entered your new password exactly the same way both times.

If you write down your password, store it in a locked place to which only you have access.

7. Tab to the *Reference Number* field and enter the reference number you obtained from your Administrator (for example, 91480170).
8. Tab to the *Authorization Code* field and enter the authorization code you obtained from your Administrator (for example, CMTJ-8VOR-VFNS). The hyphens are optional.
9. Click *OK*.

After a short period of time, the *Entrust Options* dialog appears if Entrust was able to create your Client username. The *Entrust Options* dialog contains tabs that let you choose various types of options you may want to change.



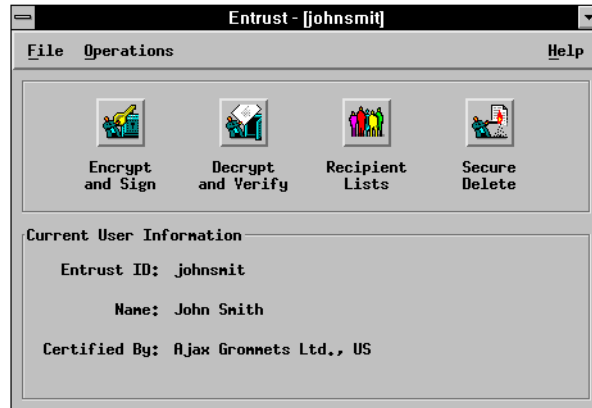
Note: If Entrust was unable to create your Client username, try supplying the information again. Ensure that you enter the reference number and authorization code in exactly the same form as that received from your Entrust Administrator. If you still cannot create a Client username, contact your Administrator.

10. Notice the *Logoff timeout* field in the *Entrust Options* dialog. This field specifies the length of time the Client will leave you logged on before automatically logging you off. This option reduces the risk of someone signing files with your digital signature or decrypting your files while you are temporarily away from your computer. You can set this number between 1 and 60 minutes. Enter a value that suits your needs.

Note: For information about the other options you can set, refer to "Setting options for Entrust/Client" on page 116.

11. Click *OK* in the *Entrust Options* dialog.

The *Entrust* main window appears. You can now begin using Entrust.



You can now encrypt, decrypt, sign, and verify files. You can also create your address book, create recipient lists, change your password and securely delete files.

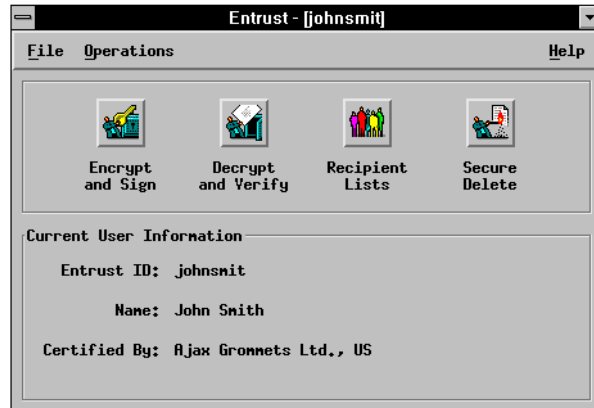
Note: If you have not already done so, destroy the reference number and authorization code you used to create your Client username.

Encrypting and signing your first files

This section shows you how to encrypt and sign one or more files. It is assumed that you are logged on; however, it is possible that you were automatically logged off. The Client has a safety feature that logs you off a preset number of minutes after you last used the Client. You can set the number of minutes in the *Entrust Options* dialog. To access the *Entrust Options* dialog, choose *Options...* from the *File* menu. If you attempt to use the Client while you are logged off, you will be automatically prompted to log on.

Decide which files to encrypt and sign, and then proceed as follows:

1. Click the *Encrypt and Sign* icon in the *Entrust* main window.



The *Select files to be encrypted and/or signed* dialog appears.



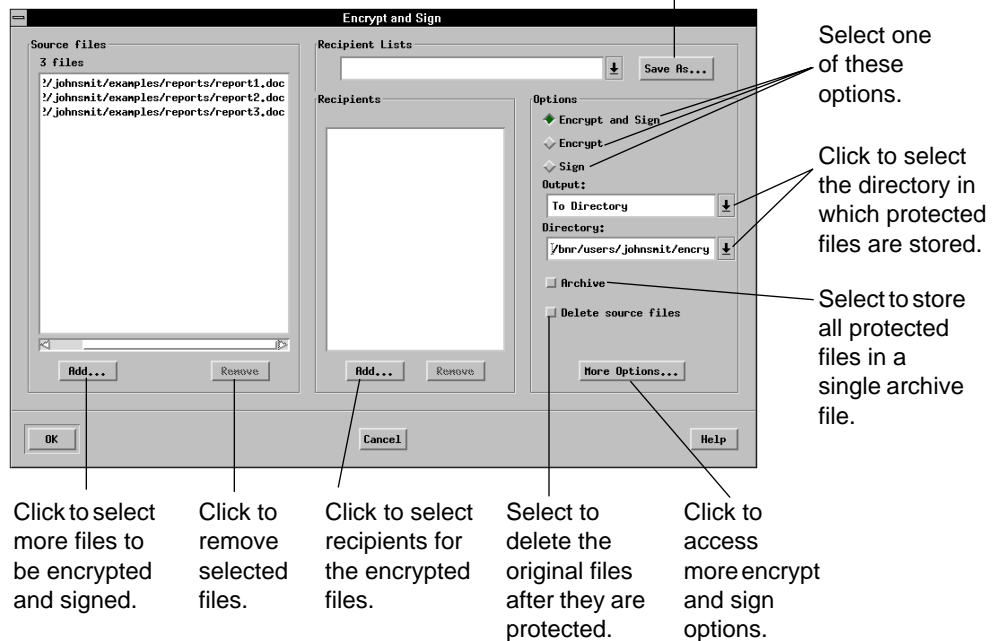
2. Navigate to the directory that contains the files you want to encrypt and sign.

To change directory, click a directory name in the *Directories* list within the *Select files to be encrypted and/or signed* dialog. Traverse branches as you would normally do in UNIX.

3. Select a single file you want to encrypt and sign by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

The *Encrypt and Sign* dialog appears displaying the names of the files you selected.

Click to save the current recipients and options in a new recipient list.



4. You may still select more files to encrypt and sign. Proceed as follows:
 - a. Click *Add...* in the *Source Files* section of the *Encrypt and Sign* dialog.

The *Select files to be encrypted and/or signed* dialog reappears.

- b. Navigate to the directory that contains the files you want to encrypt and sign.
- c. Select a single file you want to encrypt and sign by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

The *Encrypt and Sign* dialog reappears.

- d. Repeat steps 4.a. to 4.c. until you have selected all the files you require. You can select files from more than one directory.

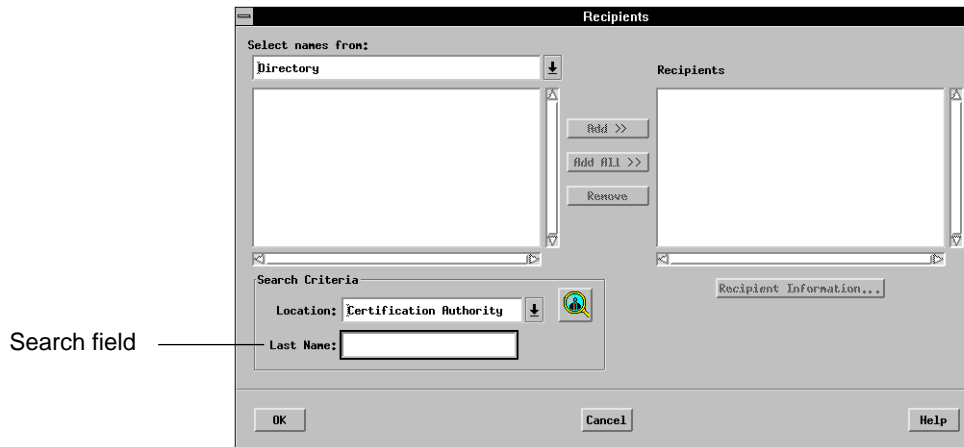
5. Select recipients for the encrypted files.

You only need to select recipients whenever you encrypt files. You do not need to select recipients if you sign files without encrypting them. You are automatically designated as a recipient of all files you encrypt. If you specify no recipients, you will be the only one who can decrypt the encrypted files.

Proceed as follows to select recipients:

- a. Click *Add...* in the *Recipients* section of the *Encrypt and Sign* dialog.

The *Recipients* dialog appears.



- b. Notice the *Location* field within the *Search Criteria* section of the *Recipients* dialog. This field is optional and only appears if your Entrust Security Officer has set up multiple search bases. If the field does not appear, do not be alarmed. The field is only useful if your system uses multiple search bases and multiple search bases are

not required in most systems. If the *Location* field does not appear, your system uses a single search base.

Multiple search bases provide a method for you to specify the user community in which to perform the search. Generally, you will want to leave the search base set to *Certification Authority* as that setting allows you to search for all other Entrust users in your CA security domain. Speak to your Entrust Administrator for more information about how to use other search bases that are set up for you.

- c. Locate the search field(s) within the *Search Criteria* section of the *Recipients* dialog.


If no search fields appear in the *Recipients* dialog, it is probably because you do not have a network connection. For more information about this situation, refer to "Search information is unavailable" on page 128.

ATTENTION

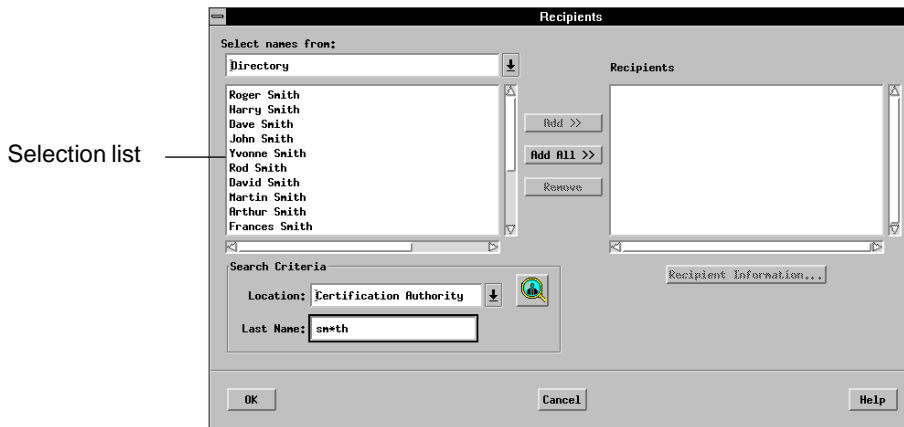
The search field(s) can vary from organization to organization. The search field(s) you see will be those that are most useful for searching the names of recipients in your organization. In this user guide, one search field (*Last Name*) is used. If you do not know how to use the search field(s), ask your Entrust Administrator.

- d. In the search field(s), enter the name of a person to whom you want to give protected files.

You can replace characters in search field(s) with the * wild card; for example, sm*th would find occurrences of smith, smooth and smyth.

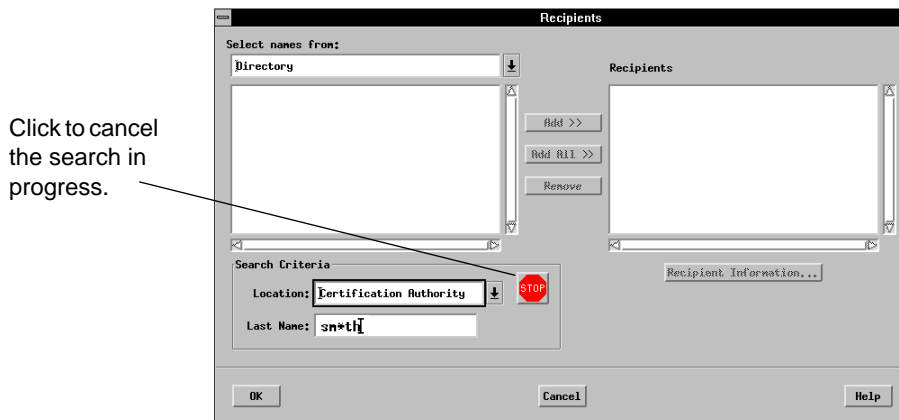
- e. Press the *Enter* key or click the *Search*  icon.

The result of the search appears in the selection list.



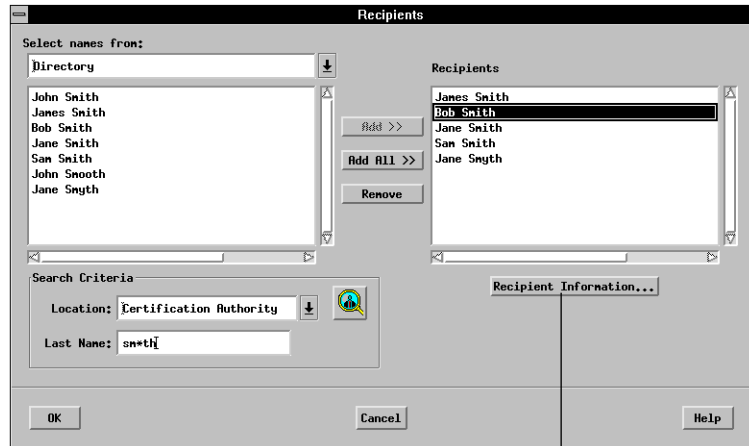
Note: There is a limit to the number of possible recipients that can be displayed in the selection list. This limit is set by the Directory Administrator. If the search information you specify is too broad, this limit may be exceeded and only a partial list will be displayed in the selection list. A message will alert you to this situation. If this occurs, return to step 5.d. and enter more specific search information (for example, if you had entered s* in the search field, you might then enter sm*th instead).

If there is heavy traffic on your network, it is possible that the search may take too long (such occurrences are rare, however). During the search, the *Search* icon changes to a *Stop Sign* icon. You can cancel the search by clicking the *Stop Sign* icon and try again later when your network is less busy.



- f. Select the names of the recipients you want from the selection list and click *Add>>*. Alternatively, you can double-click the names of the recipients you want. You can also select all the names from the selection list by clicking *Add All>>*.

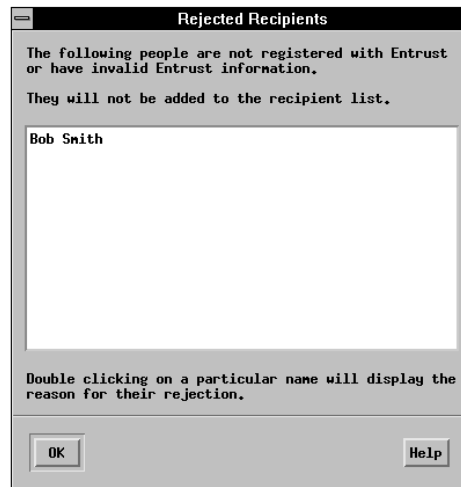
The names of the recipients you select from the selection list appear in the *Recipients* section of the *Recipients* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.



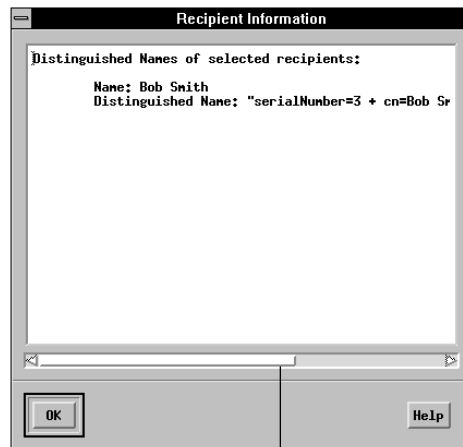
Click to display information about the currently selected recipient.

Note: If the *Rejected Recipients* dialog appears when you select names from the selection list, it means that the Client cannot encrypt files for the recipients shown in the dialog. Click *OK* and continue the procedure. If you want to know why the Client cannot encrypt files for

a rejected recipient, double-click the recipient's name in the list. Click OK to leave the *Rejected Recipients* dialog.



- g. You can display information about a recipient by selecting the recipient's name in the *Recipients* dialog and clicking *Recipient Information...*



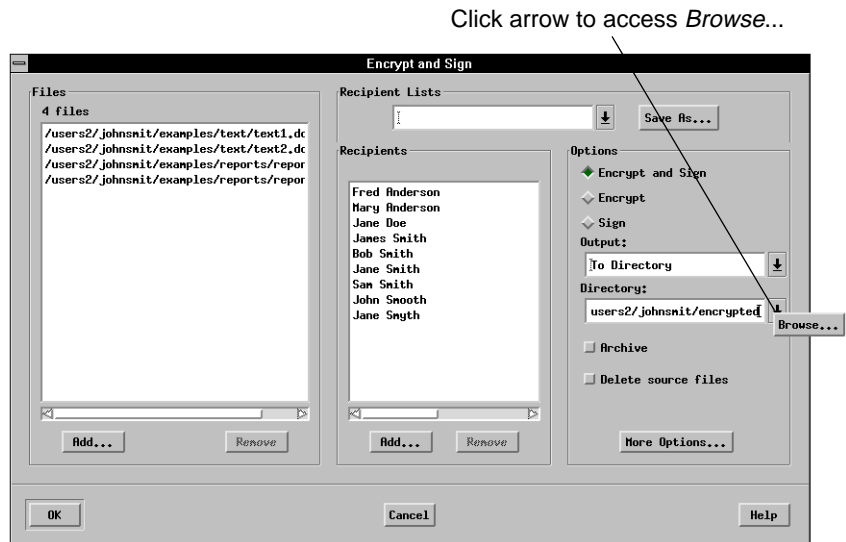
Use the scroll bar to view all of the information.

- h. You can remove recipients individually from the *Recipients* section of the *Recipients* dialog by double-clicking them. Alternatively, you can select the recipients you want to remove by clicking each recipient

while holding down the *Shift* or the *Ctrl* key and then clicking *Remove*.

- i. If you want to search for more recipients, return to step 5.d.
- j. Once you have selected all the recipients you want, click *OK* in the *Recipients* dialog.

The *Encrypt and Sign* dialog reappears displaying the names of the recipients you selected.



6. Select the *Encrypt and Sign* option to include your digital signature with the encrypted files.

Note: Most options you select remain in effect until you change them again; there are no default settings. For example, if you select the *Sign* option, the next time you display the *Encrypt and Sign* dialog, the *Sign* option will still be selected.

7. Notice the *Output* field and the *Directory* field.

You have different options when deciding where to output your encrypted and signed files. For now, set the *Output* field to *To Directory*.

When you protect a file, the Client stores the protected file in the directory that you specify in the *Directory* field. This directory selection remains in effect until you change it. Note that the original, unprotected file is left intact (unless you select the *Delete source files* option).

8. In the *Directory* field, enter the full path to the directory in which you want to store your encrypted and signed files (for example, *encrypted* directory in your home directory). If the directory does not already exist, you will be prompted to create it.

Alternatively, you can use *Browse...* to locate and select an existing directory in which to store your encrypted and signed files.

The *Directory* field and *Browse...* are only available when the *Output* field is set to *To Directory*; however, the directory you specify in the *Directory* field will remain in effect until you change it again.

9. For now, leave the *Archive* option unselected.

The *Archive* option causes all the encrypted and signed files to be stored in a single archive file. This is useful if you want to transfer several protected files; by storing all the protected files in a single archive file, you only need to transfer a single file. When the archive file is decrypted, the original files will be restored with their original filenames.

10. If you want to display other encrypt and sign options, click *More Options...* Refer to "Encrypt and sign options" on page 117 for more information about these options.

11. Review the files, recipients and options you have selected. You can still make changes. You can add and/or remove files and/or recipients, and you can select different options.

12. Once you are satisfied with your selections, you are ready to begin the encryption and signature process. However, at this time you have the option to save the current recipients and options in a *recipient list* for reuse later.

Recipient lists provide an express mechanism to select recipients and options when you protect files. Instead of having to specify each recipient and option every time you want to protect files, you can simply select the name of a *recipient list* with a single mouse-click. You control who is part of a recipient list and you can create more than one recipient list. For example, you could create one recipient list for each project you work on. Note that a recipient can be a member of more than one *recipient list*. Refer to "Using saved lists of recipients" on page 93 for more information.

To save the current recipients and options in a recipient list, proceed as follows:

- a. Click *Save As...* in the *Encrypt and Sign* dialog.

The *Recipient List* dialog appears.

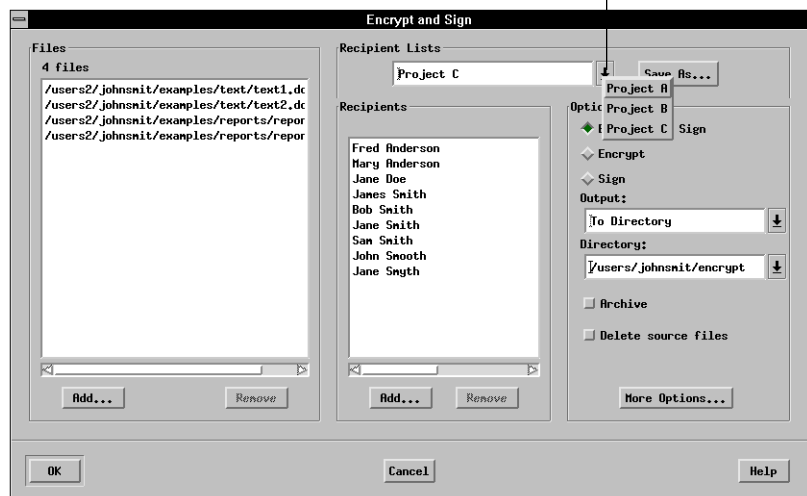


- b. Enter the name of the recipient list. This is the name that will appear in the *Recipient Lists* field at the top of the *Encrypt and Sign* dialog.
- c. Click *OK*.

The *Encrypt and Sign* dialog reappears.

- d. Click the *Recipient Lists* pull-down list to see the names of all the recipient lists you have created.

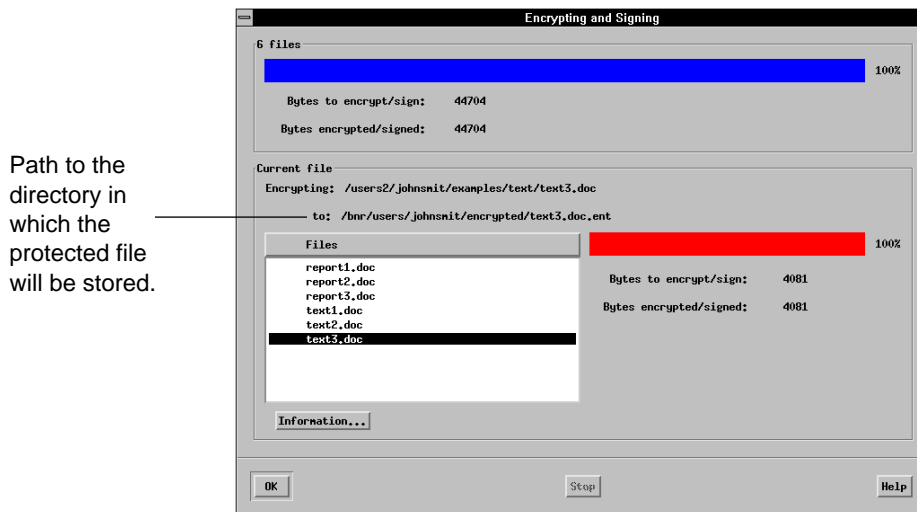
Click to display existing recipient lists.



The next time you need to encrypt and/or sign files, you can use the recipient list you just created to quickly specify recipients and options.

- 13. Click *OK* in the *Encrypt and Sign* dialog to encrypt and sign the files you selected.

The *Encrypting and Signing* dialog appears, and the files are encrypted and signed.



14. Click **OK** in the *Encrypting and Signing* dialog once the files are encrypted and signed.

The *Entrust* main window reappears.

The files you selected are now securely protected and stored in the directory you specified in the *Directory* field in the *Encrypt and Sign* dialog. If you look in that directory, you will notice that the files you protected have the default *ent* filename extension; for example, if you protected a file called *report7.doc*, the filename of the protected file is *report7.doc.ent*. You can specify a different filename extension as explained in “Encrypt and sign options” on page 117.

You can now give the protected files to your chosen recipients. No one other than the chosen recipients and you will be able to decrypt the files.

You will notice a slight increase in the size of files after you encrypt and/or sign them. The size of a protected file depends on whether the file is only encrypted, only signed, or both encrypted and signed. The size of the protected file increases slightly for each recipient you include.

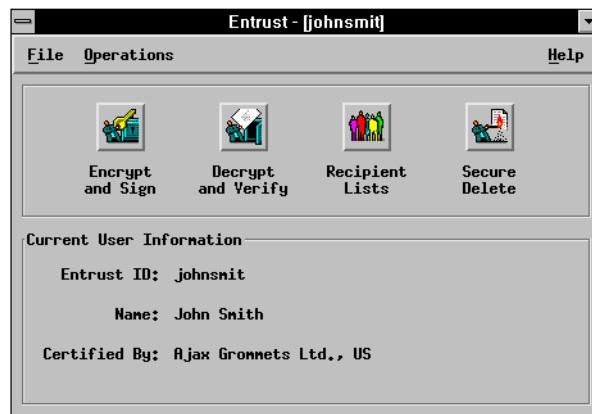
ATTENTION

It is critical that you do not make changes to protected files. Even the slightest change to the files will cause corruption and make it impossible to decrypt and verify them at a later time.

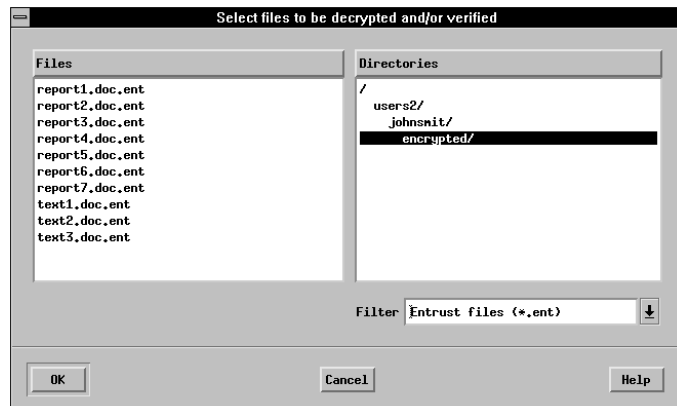
Decrypting and verifying your first protected files

In this section, you will decrypt and verify the files you just protected. Proceed as follows:

1. Click the *Decrypt and Verify* icon in the *Entrust* main window.



The *Select files to be decrypted and/or verified* dialog appears.

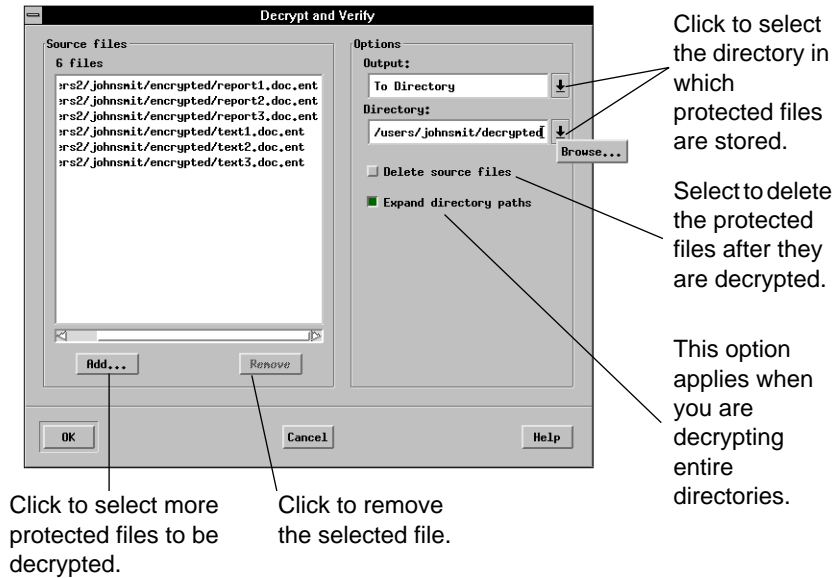


2. Navigate to the directory that contains the files you want to decrypt and verify.

To change directory, click a directory name in the *Directories* list within the *Select files to be decrypted and/or verified* dialog. Traverse branches as you would normally do in UNIX.

3. Select a single file you want to decrypt and verify by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

The *Decrypt and Verify* dialog appears.



4. Notice the *Output* field and the *Directory* field.

You have different options when deciding where to store your unprotected files. For now set the *Output* field to *To Directory*. When you decrypt and/or verify a file, the Client stores the unprotected file in the directory that you specify in the *Directory* field. This directory selection remains in effect until you change it. The *Directory* field only appears if the *Output* field is set to *To Directory*. Note that the protected file is left intact.

5. In the *Directory* field, enter the path to the directory in which you want to store your decrypted file. If the directory does not already exist, you will be prompted to create it.

Alternatively, you can use *Browse...* to locate and select an existing directory in which to store your decrypted file.

The *Directory* field and *Browse...* are only available when the *Output* field is set to *To Directory*; however, the directory you specify in the *Directory* field will remain in effect until you change it again.

6. You may select more files to unprotect. Proceed as follows:

- a. Click *Add...* in the *Source files* section of the *Decrypt and Verify* dialog.

The *Select files to be decrypted and/or verified* dialog reappears.

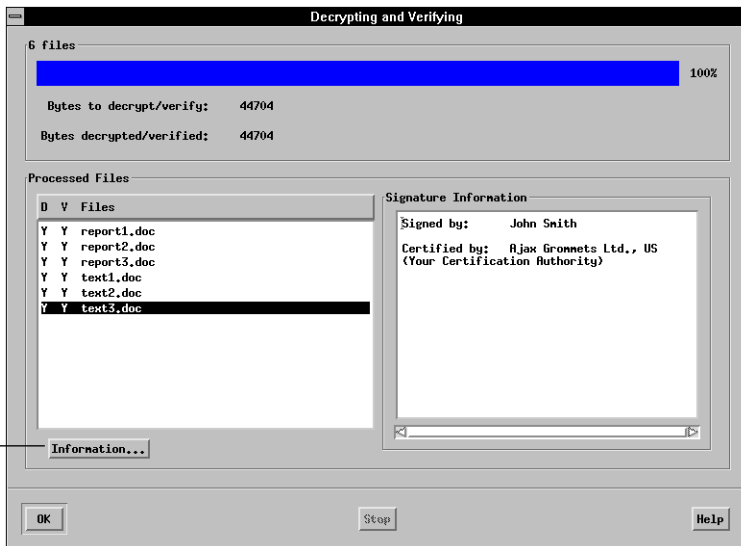
- b. Navigate to the directory that contains the files you want to decrypt and verify.
- c. Select a single file you want to decrypt and verify by double-clicking it. Alternatively, you can select several files by clicking each one while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.
- d. Repeat steps 6.a. to 6.c. until you have selected all the files you require. You can select files from more than one directory.

Once you have selected the files you want to decrypt, you are ready to begin the decryption and verification process.

7. Click *OK* in the *Decrypt and Verify* dialog.

The *Decrypting and Verifying* dialog appears.

Click to display
information
about the
selected file.



The capital Y (yes) in the column headed by the capital D (decrypt) means the file was decrypted. The capital Y in the column headed by the capital V (verify) means that the signature with the file was verified.

D	V	Files
Y	Y	report3.doc

The *Signature Information* section of the *Decrypting and Verifying* dialog shows the name of the person who signed the file (in this case yourself) and the name of the Certification Authority that certified your signature.

The Certification Authority comprises one or more people who are responsible for security policy decisions in your organization.

8. Click *OK* to leave the *Decrypting and Verifying* dialog.

The *Entrust* main window reappears.

The decrypted file is stored in the directory that was specified by the *Directory* field in the *Decrypt and Verify* dialog. You can open, move, and rename this file.

Ending your Entrust/Client session

To end your Client session, choose *Exit* from the *File* menu.

Using Entrust/Client

This chapter provides step-by-step procedures for Entrust/Client functions. Most of these procedures assume the following:

- The Client was successfully installed.
- You have created your Client username.
- The Client is running.

Note: If the Client is not already running, refer to “Starting Entrust/Client for the first time” on page 26.

Most of the procedures in this chapter also assume that you are logged on to the Client; however, it is possible that you were automatically logged off. Entrust has a safety feature that logs you off a preset number of minutes after you last used the Client. You can set the number of minutes in the *Entrust Options* dialog. To access the *Entrust Options* dialog, choose *Options...* from the *File* menu. If you attempt to use the Client while you are logged off, you will automatically be prompted to log on.

Protecting the contents of your files

You can protect the contents of your files from intruders by encrypting them using Entrust/Client. Once encrypted, these files cannot be read by anyone (including you) until they are decrypted.

You can distribute encrypted files to the recipients of your choice with complete confidence that only they can decrypt them.

You can provide your recipients with additional assurance by digitally signing the protected files. Your digital signature guarantees that the files came from you and that they were not altered since you sent them.

To protect the contents of your files, complete the following steps:

- Select the files you want to encrypt and/or sign.
- Select recipients for the encrypted files (you do not need to select recipients for files that are signed but not encrypted).
- Select options for the encrypted and/or signed files.
- Save current recipients and options in a recipient list. This step is optional.
- Encrypt and/or sign the files.

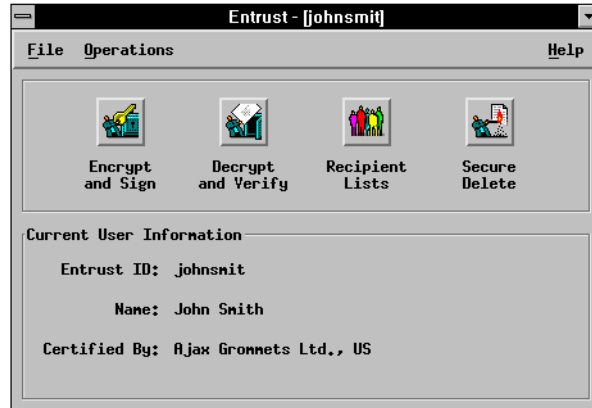
Each of these steps is described in detail in the following sections.

Selecting files to encrypt and sign

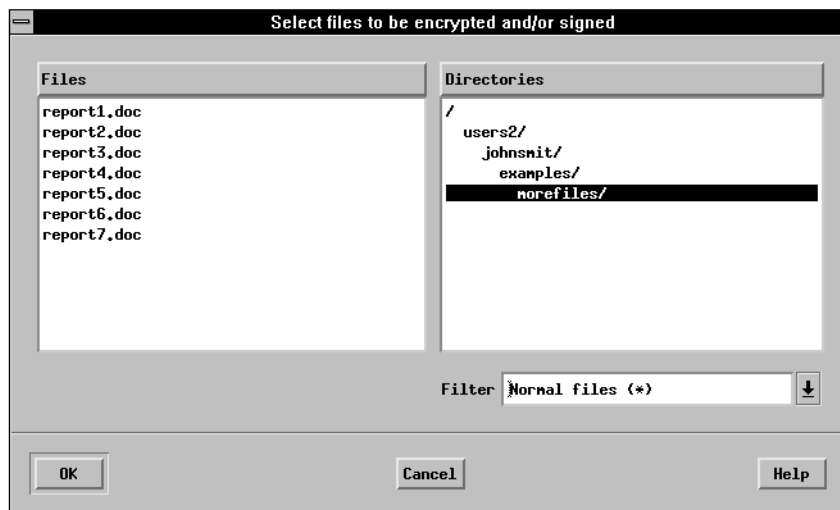
This section describes how to select the files you want to encrypt and/or sign. Each of the files you select for protection is encrypted for the same set of recipients.

Before you can access the *Encrypt and Sign* dialog, you need to select files to be encrypted and/or signed. Proceed as follows:

1. Click the *Encrypt and Sign* icon in the *Entrust* main window.

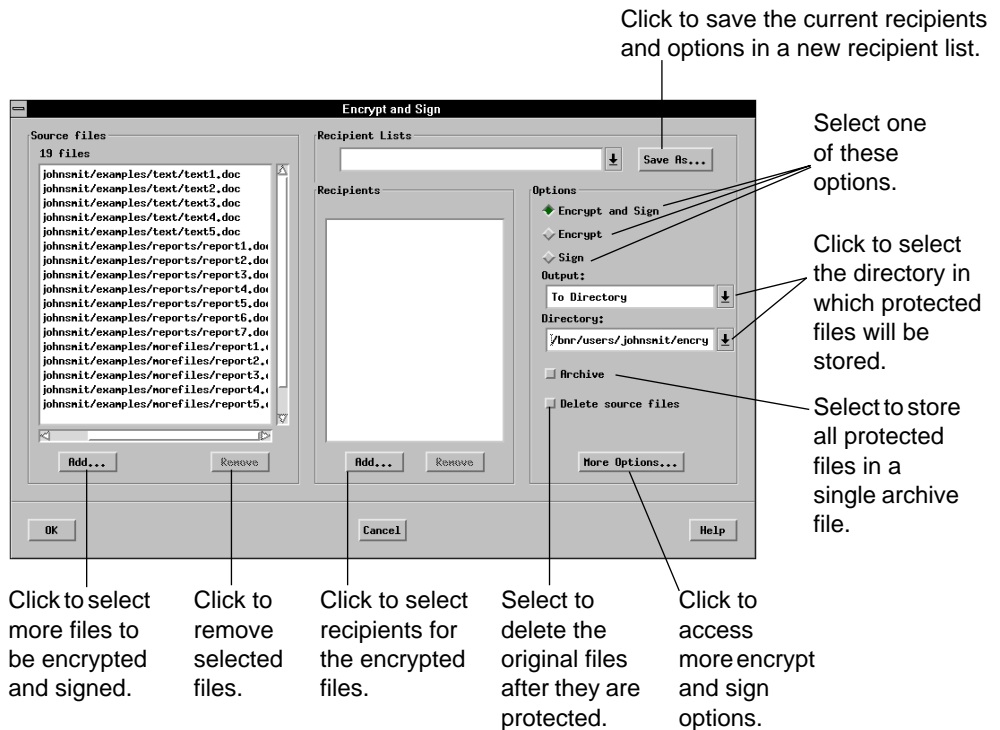


The following dialog appears.



2. Navigate to the directory that contains the files you want to encrypt and sign.
To change directory, click a directory name in the *Directories* list within the *Select files to be encrypted and/or signed* dialog. Traverse branches as you would normally do in UNIX.
3. Select a single file you want to encrypt and sign by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

The *Encrypt and Sign* dialog appears displaying the names of the files you selected.



4. You may still select more files to encrypt and sign. Proceed as follows:
 - a. Click *Add...* in the *Source files* section of the *Encrypt and Sign* dialog.

The *Select files to be encrypted and/or signed* dialog reappears.
 - b. Navigate to the directory that contains the files you want to encrypt and sign.
 - c. Select a single file you want to encrypt and sign by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

The *Encrypt and Sign* dialog reappears.
 - d. Repeat steps 4.a. to 4.c. until you have selected all the files you require. You can select files from more than one directory.

Now you should select recipients for your encrypted files. Refer to “Selecting recipients for your encrypted files” below for more information. If you want to encrypt a file so that only you can decrypt it, you do not need to select any recipients. Also, if you only want to sign files, you do not need to select recipients. In this case, refer to “Selecting encrypting and signing options” on page 66 for information about selecting options.

Selecting recipients for your encrypted files

Recipients are the people whom you authorize to decrypt your protected files. You only need to select recipients for encrypted files. If you sign files without encrypting them, there is no need to specify recipients. Note that you are automatically designated as a recipient for each file you encrypt; therefore, you do not have to specify yourself as a recipient.

You can select recipients for encrypted files in the following ways:

- by selecting an existing recipient list from the *Encrypt and Sign* dialog (see “Selecting an existing recipient list from the Encrypt and Sign dialog” on page 61)
- by selecting an existing recipient list from the *Recipients* dialog (see “Selecting an existing recipient list from the Recipients dialog” on page 63)
- by searching for the names of people (see “Selecting recipients by name” on page 52)
- by selecting people from your address book (see “Selecting recipients by name in personal address book” on page 57)
- any combination of the above

Selecting recipients by name

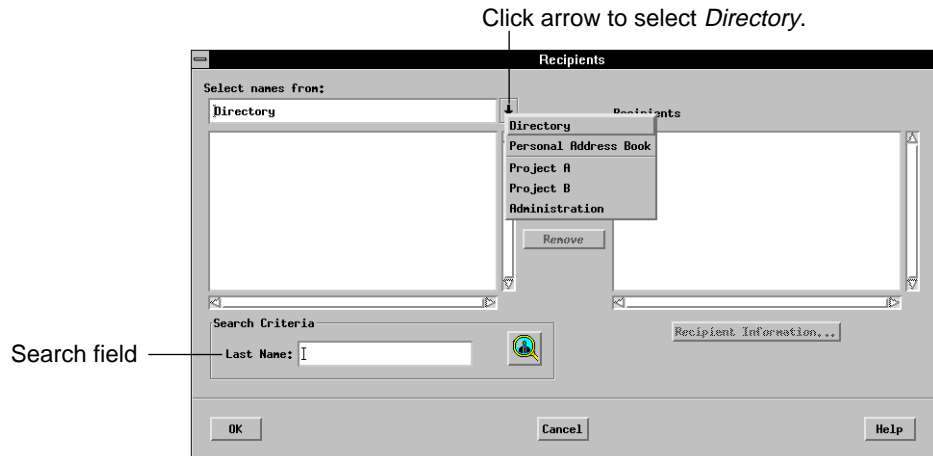
This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to “Selecting files to encrypt and sign” on page 48.

To select recipients by name, proceed as follows:

1. Select *To Directory* or *In Place* from the *Output* pull-down list in the *Encrypt and Sign* dialog.
2. Click *Add...* at the bottom of the *Recipients* section in the *Encrypt and Sign* dialog.

The *Recipients* dialog appears.

3. Select *Directory* from the *Select names from* pull-down list at the top of the *Recipients* dialog.



4. Locate the search field(s) within the *Search Criteria* section.

If no search field appears in the dialog, it is probably because you do not have a network connection. If you do not have a network connection, the contents of your address book (if you have one) will appear automatically in the selection list. For more information about this situation, refer to “Search information is unavailable” on page 128.

ATTENTION

The search field(s) can vary from organization to organization. The search field(s) you see will be those that are most useful for searching the names of recipients in your organization. In this user guide, one search field (*Last Name*) is used. If you do not know how to use the search field(s), ask your Entrust Administrator.

5. In the search field(s), enter the name of a person to whom you want to give protected files.

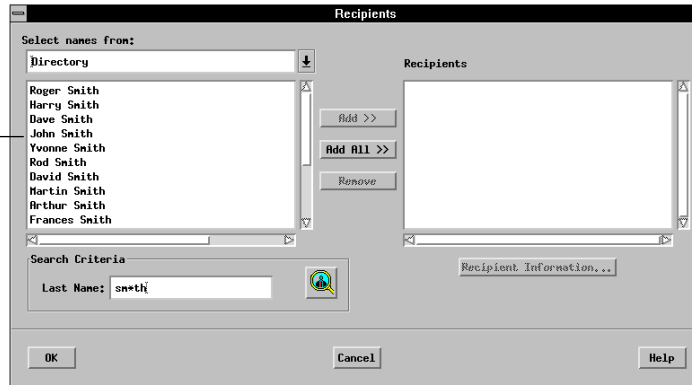
You can replace characters in the search field(s) with the * wild card; for example, sm*th would find occurrences of smith, smooth and smyth.



6. Press the *Enter* key or click the *Search* icon.

The result of the search appears in the selection list.

Selection list

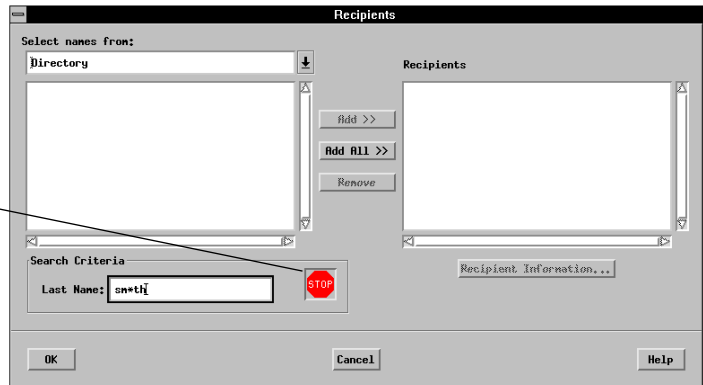


Note: There is a limit to the number of possible recipients that can be displayed in the selection list. If the search information you specify is too broad, this limit may be exceeded and only a partial list will be displayed in the selection list. A message will alert you to this situation. If this occurs, return to step 5. and enter more specific search information (for example, if you had entered s* in the search field, you might then enter sm*th instead).

If there is heavy traffic on your network, it is possible that the search may take too long (such occurrences are rare, however). During the search, the

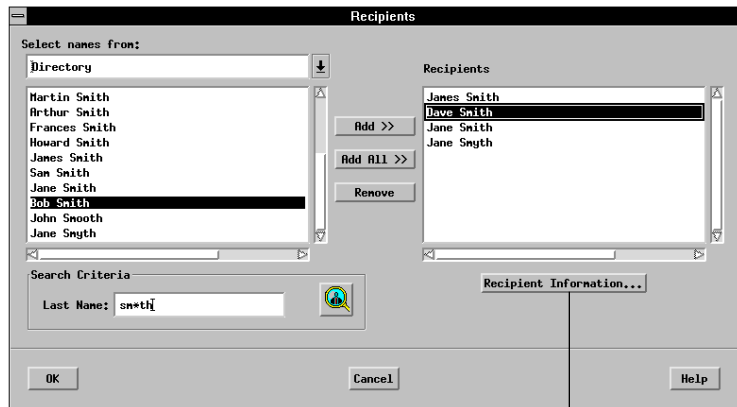
Search icon changes to a *Stop Sign* icon. You can cancel the search by clicking the *Stop Sign* icon.

Click to cancel the search in progress.



7. Select the names of the recipients you want from the selection list and click *Add >>*. Alternatively, you can double-click the names of the recipients you want. You can also select all the names from the selection list by clicking *Add All >>*.

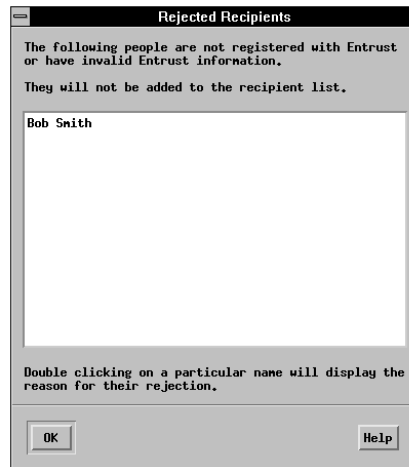
The names of the recipients you select from the selection list appear in the *Recipients* section of the *Recipients* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.



Click to display information about the currently selected recipient.

Note: If the *Rejected Recipients* dialog appears when you select names from the selection list, it means that the Client cannot encrypt files for the recipients shown in the dialog. Click *OK* and continue the procedure. If you want to know why the Client cannot encrypt files for a rejected

recipient, double-click the recipient's name in the list of names. Click *OK* to leave the *Rejected Recipients* dialog.



8. You can display information about a recipient by selecting the recipient's name and clicking *Recipient Information...*

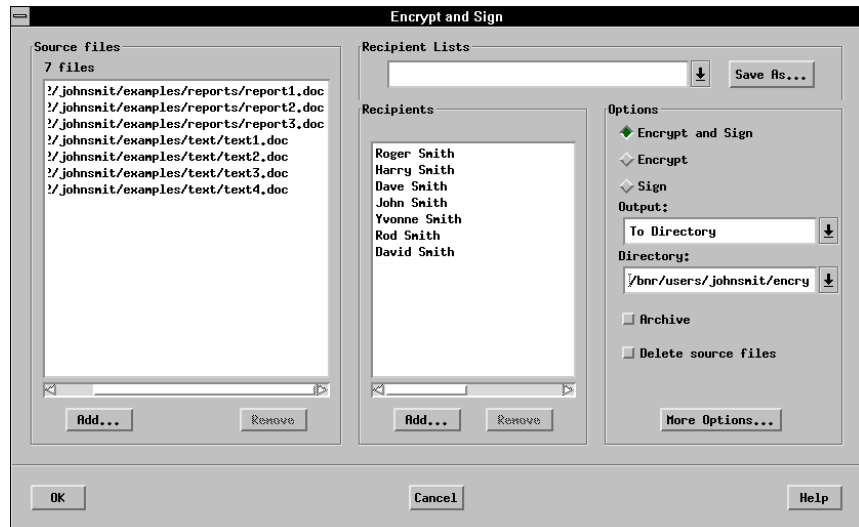


Use the scroll bar to view all of the information.

9. You can remove recipients individually from the *Recipients* section of the *Recipients* dialog by double-clicking them. Alternatively, you can select the recipients you want to remove by clicking each recipient while holding down the *Shift* or the *Ctrl* key and then clicking *Remove*.
10. If you want to include more recipients by name, return to step 5.

11. Once you have selected all the recipients you want, click *OK* to leave the *Recipients* dialog.

The *Encrypt and Sign* dialog reappears displaying the names of the recipients you selected.



12. You can add more recipients using one of the methods explained in “Selecting recipients for your encrypted files” on page 51.

You can remove recipients from the *Recipients* section of the *Encrypt and Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

Now you can specify encrypting and signing options. Refer to “Selecting encrypting and signing options” on page 66.

Selecting recipients by name in personal address book

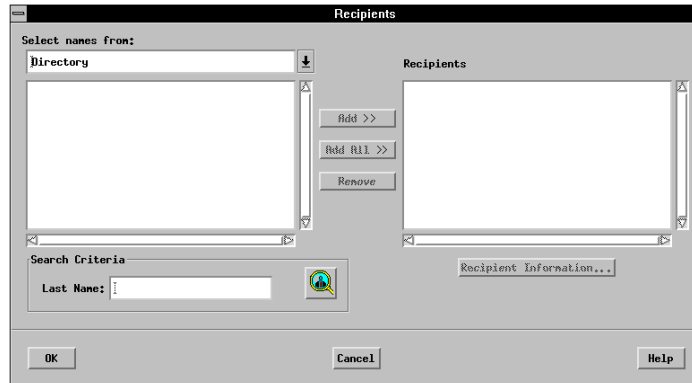
This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to “Selecting files to encrypt and sign” on page 48.

You can specify recipients by selecting names from your personal address book.

To select recipients from your address book, proceed as follows:

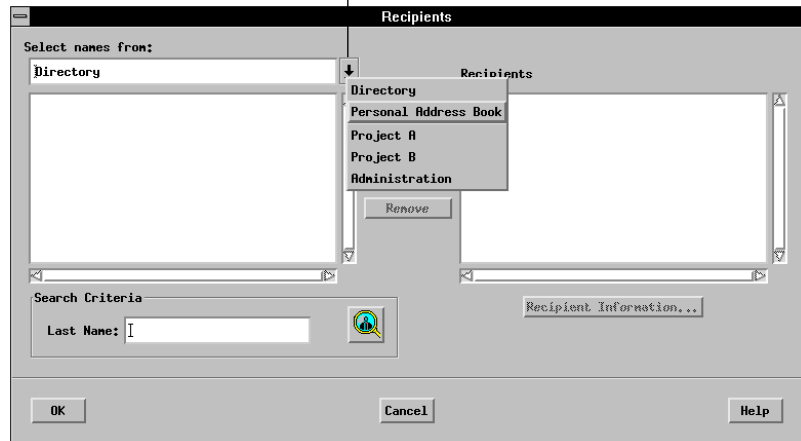
1. Select *To Directory* or *In Place* from the *Output* pull-down list in the *Encrypt and Sign* dialog.
2. Click *Add...* at the bottom of the *Recipients* section in the *Encrypt and Sign* dialog.

The *Recipients* dialog appears.



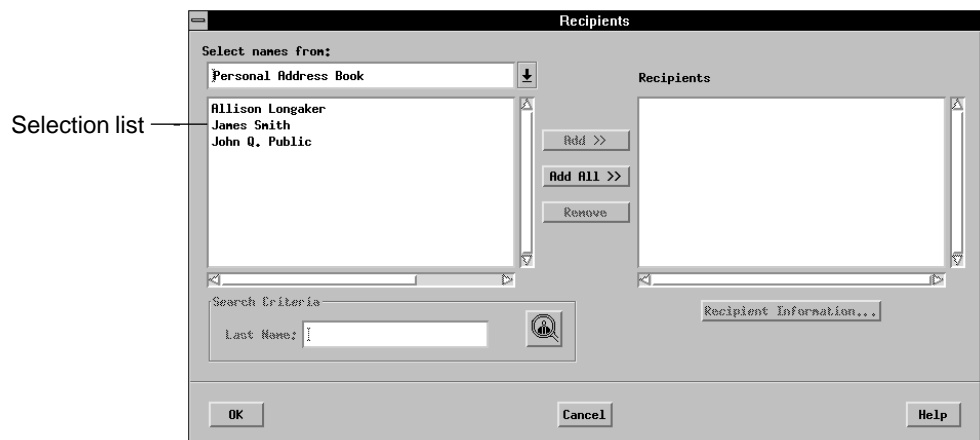
3. Select *Personal Address Book* from the *Select names from* pull-down list at the top of the *Recipients* dialog.

Click arrow to select *Personal Address Book*.



Note: If *Personal Address Book* does not appear in the *Select names from* pull-down list at the top of the *Recipients* dialog, you have not yet created an address book. For information about address books, refer to “Creating and accessing your address book” on page 84.

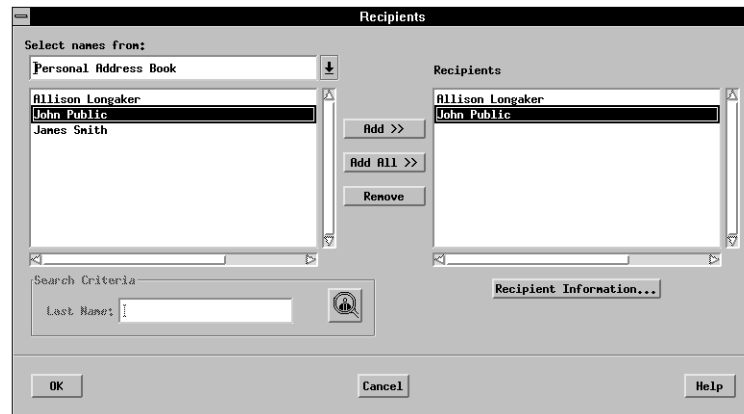
The names in your address book appear in the selection list.



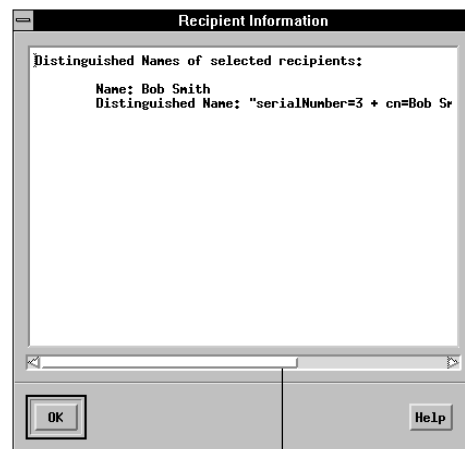
4. Select the names of the recipients you want from the selection list and click *Add >>*. Alternatively, you can double-click the names of the

recipients you want. You can also select all the names from the selection list by clicking *Add All >>*.

The names of the recipients you select from the selection list appear in the *Recipients* section of the *Recipients* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.



5. You can display information about a recipient by selecting the recipient's name and clicking *Recipient Information...*



Use the scroll bar to view all of the information.

6. You can remove recipients individually from the *Recipients* section of the *Recipients* dialog by double-clicking them. Alternatively, you can select the

recipients you want to remove by clicking each recipient while holding down the *Shift* or the *Ctrl* key and then clicking *Remove*.

7. Once you have selected all the recipients you want, click *OK* to leave the *Recipients* dialog.

The *Encrypt and Sign* dialog reappears displaying the names of the recipients you selected.



8. You can add more recipients using one of the methods explained in “Selecting recipients for your encrypted files” on page 51.

You can remove recipients from the *Recipients* section of the *Encrypt and Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

Now you can specify encrypting and signing options. Refer to “Selecting encrypting and signing options” on page 66.

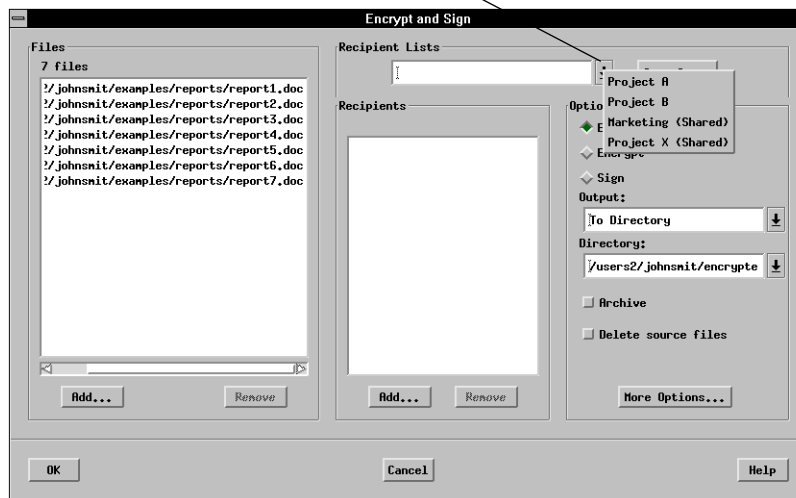
Selecting an existing recipient list from the Encrypt and Sign dialog

This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to “Selecting files to encrypt and sign” on page 48. This section also assumes that you have already created at least one recipient list. If you have not yet created a recipient list, refer to “Using saved lists of recipients” on page 93.

From the *Encrypt and Sign* dialog, you can specify recipients by selecting members of one of your existing recipient lists. Proceed as follows:

1. Select the name of the recipient list you want from the *Recipient Lists* pull-down list at the top of the *Encrypt and Sign* dialog.

Click arrow to select a recipient list (if you previously created one).



Note: If no recipient lists appear in the *Recipient Lists* pull-down list, you have not yet created a recipient list. For information about recipient lists, refer to “Using saved lists of recipients” on page 93.

The names of the people who are members of the recipient list you selected appear in the *Recipients* section of the *Encrypt and Sign* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.

Notice that some options may have changed in the *Encrypt and Sign* dialog when you selected a recipient list because recipient lists store a set of recipient names and options.

Note: If the *Rejected Recipients* dialog appears when you select a shared recipient list, it is likely that some of the recipients in the shared recipient list came from the recipient list originator's personal address book. Before you can encrypt files for those recipients, you must import their Entrust addresses into your own personal address book.

2. You can add more recipients using one of the methods explained in "Selecting recipients for your encrypted files" on page 51.

You can remove recipients from the *Recipients* section of the *Encrypt and Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

If you make changes to the recipients or to the options, you can save them in a new recipient list by clicking *Save As...* at the top of the *Encrypt and Sign* dialog.

Now you can specify encrypting and signing options. Refer to "Selecting encrypting and signing options" on page 66.

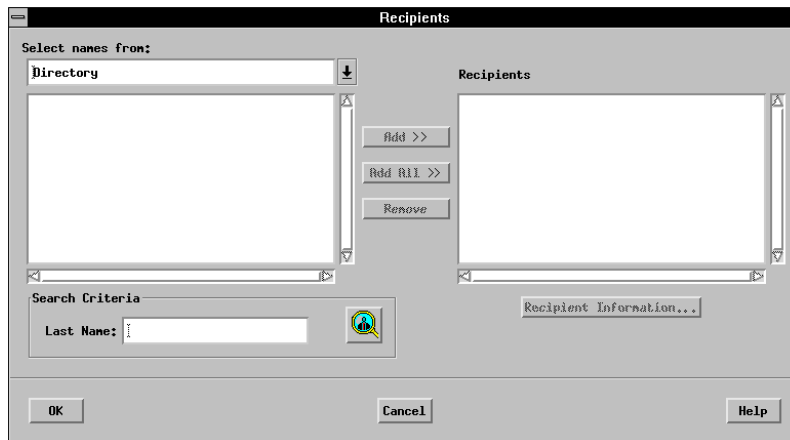
Selecting an existing recipient list from the Recipients dialog

This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to “Selecting files to encrypt and sign” on page 48. This section also assumes that you have already created at least one recipient list. If you have not yet created a recipient list, refer to “Using saved lists of recipients” on page 93.

From the *Recipients* dialog, you can specify recipients by selecting members of one of your existing recipient lists. Proceed as follows:

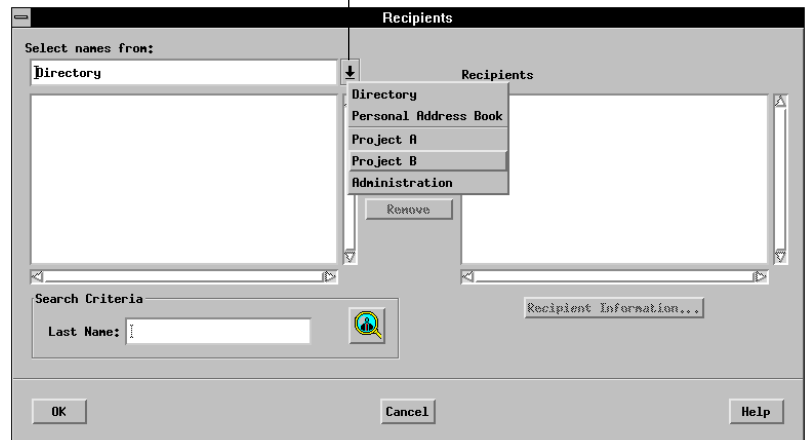
1. Select *To Directory* or *In Place* from the *Output* pull-down list in the *Encrypt and Sign* dialog.
2. Click *Add...* at the bottom of the *Recipients* section in the *Encrypt and Sign* dialog.

The *Recipients* dialog appears.



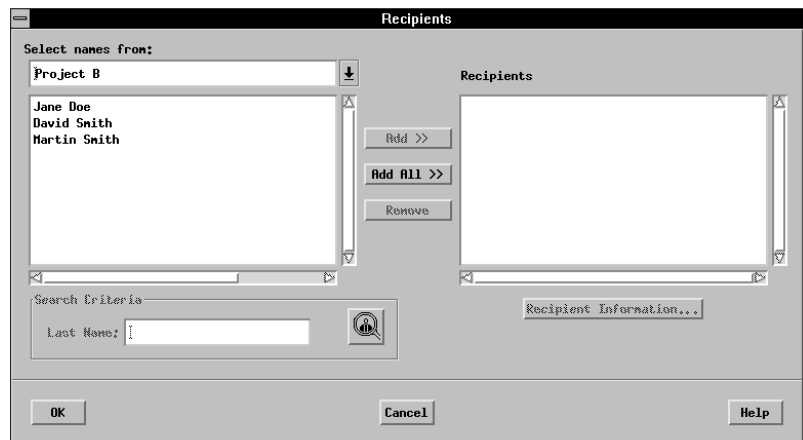
3. Select the name of the recipient list you want from the *Select names from* pull-down list at the top of the *Recipients* dialog.

Click arrow to select a recipient list.



Note: If no recipient lists appear in the *Select names from* pull-down list, you have not yet created a recipient list. For information about recipient lists, refer to “Using saved lists of recipients” on page 93.

The names of the people who are members of the recipient list you selected appear in the selection list.

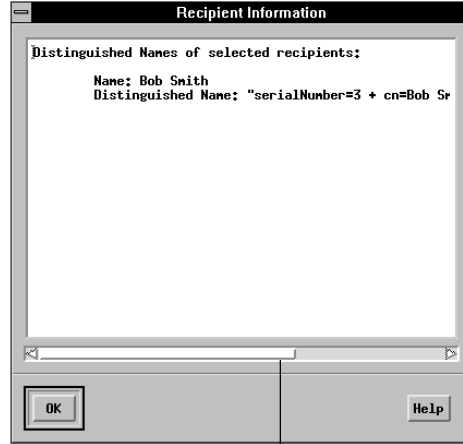


4. Select the names of the recipients you want from the selection list and click *Add >>*. Alternatively, you can double-click the names of the

recipients you want. You can also select all the names from the selection list by clicking *Add All >>*.

The names of the recipients you select from the selection list appear in the *Recipients* section of the *Recipients* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.

5. You can display information about a recipient by selecting the recipient's name and clicking *Recipient Information...*



Use the scroll bar to view all of the information.

6. You can remove recipients individually from the *Recipients* section of the *Recipients* dialog by double-clicking them. Alternatively, you can select the recipients you want to remove by clicking each recipient while holding down the *Shift* or the *Ctrl* key and then clicking *Remove*.
7. Once you have selected all the recipients you want, click *OK* to leave the *Recipients* dialog.

The *Encrypt and Sign* dialog reappears displaying the names of the recipients you selected.

8. You can add more recipients using one of the methods explained in "Selecting recipients for your encrypted files" on page 51.

You can remove recipients from the *Recipients* section of the *Encrypt and Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

If you make changes to the recipients or to the options, you can save them in a new recipient list by clicking *Save As...* at the top of the *Encrypt and Sign* dialog.

Now you can specify encrypting and signing options. Refer to “Selecting encrypting and signing options” on page 66.

Selecting encrypting and signing options

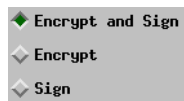
Once you have selected files to be protected and recipients (if necessary), you can choose options. If you selected a recipient list from the *Encrypt and Sign* dialog, then the options are automatically set; however, you can change those settings for this particular encrypt and/or sign operation.

This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to “Selecting files to encrypt and sign” on page 48.

When you select options, they remain selected until you change them again; Entrust remembers the settings you specify. However, option settings may change when you select a recipient list because recipient lists store recipient names and options.

To select encrypting and signing options, proceed as follows:

1. From the *Encrypt and Sign* dialog, select one of the following options:



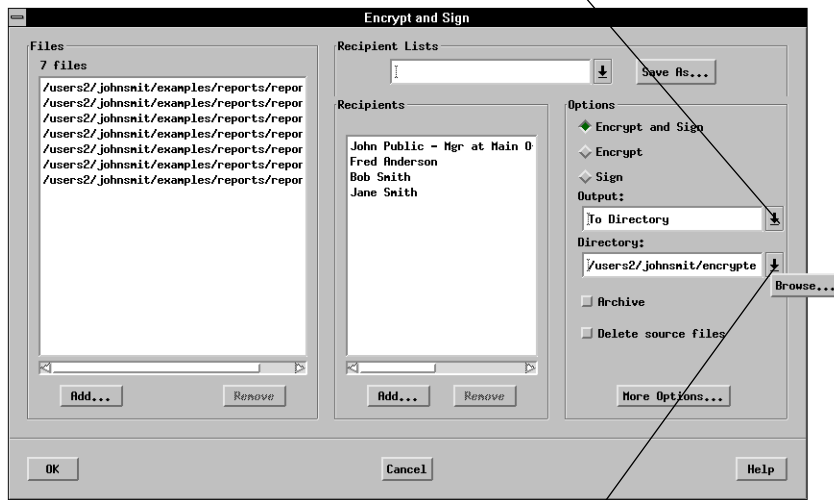
Select *Encrypt and Sign* to encrypt and sign the selected files.

Select *Encrypt* to encrypt the selected files without including your signature.

Select *Sign* to include your signature with the selected files. The files will not be encrypted. You would select this option if you were sending out information that is well known (hence it does not need to be encrypted), but you want your recipients to be assured that the information originated from you and that it has not been tampered with since you signed it.

2. Notice the *Output* field.

Click arrow to display all output options.

Click arrow to access *Browse...*

The *Output* field determines where the protected files will be stored. Valid settings are as follows:

- To Directory
- In Place

Select *To Directory* to store the protected files in the directory specified in the *Directory* field. When you protect a file, the Client stores the protected file in the directory that you specify in the *Directory* field. This directory selection remains in effect until you change it. The *Directory* field only appears if the *Output* field is set to *To Directory*. Note that the original, unprotected file is left intact.

Select *In Place* to store the protected files in the same directories as the original unprotected files. This option will also work if you select files from different directories.

3. In the *Directory* field, enter the full path to the directory in which you want to store the encrypted and signed files. If the directory does not already exist, you will be prompted to create it.

Alternatively, you can use *Browse...* to locate and select an existing directory in which to store your encrypted and signed files.

The *Directory* field and *Browse...* are only available when the *Output* field is set to *To Directory*; however, the directory you specify in the *Directory* field will remain in effect until you change it again.

4. Notice the *Archive* selection box in the *Encrypt and Sign* dialog.

Use the *Archive* option if you want to store all the encrypted and signed files in a single archive file. This is useful if you want to transfer several protected files; by storing all the protected files in a single archive file, you only need to transfer a single file. When the file is received at the intended destination and decrypted, the original files will be restored with their original filenames.

When you select *Archive*, a data entry field appears next to the *Archive* option. Enter a filename (without a filename extension) for the archive file in the *Archive* data entry field (for example, *project1*). The *Archive* option is only available when the *Output* field is set to *To Directory*. The *Archive* option does not remain selected after you leave the *Encrypt and Sign* dialog.

5. Notice the *Delete source files* selection box in the *Encrypt and Sign* dialog.

Select *Delete source files* to automatically delete the original files after they are protected. If you do not select this option, the original, unprotected files will remain intact after a copy of each file is protected.

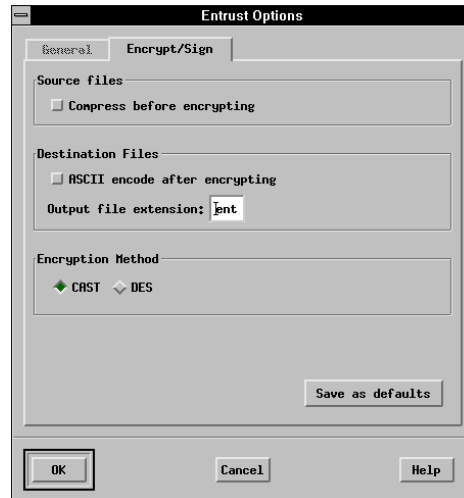
ATTENTION

Delete source files is a true delete. This means that the original file for each file you protect is completely unrecoverable using any file-recovery utility. This prevents anyone from searching your hard disk for the original file after you have protected it. The only way you will be able to recover the original file is by decrypting the protected output file. Therefore, if you use the *Delete source files* option, ensure that you do not delete the protected file.

You can, if you wish, use the Secure Delete function to delete the original, unprotected files from your system in a way that the files are completely unrecoverable using any file-recovery utility. Refer to "Deleting files so that they are unrecoverable" on page 73.

6. Click *More Options...* in the *Encrypt and Sign* dialog.

The *Entrust Options* dialog for encrypting and signing appears.



Encrypt and sign options you can select are as follows:

- Compress before encrypting
- ASCII encode after encrypting
- Output file extension
- Encryption Method

Select *Compress before encrypting* to compress the files before they are protected. It is necessary to compress files before they are encrypted because it is impossible to compress an encrypted file. By definition, an encrypted file is completely random, making compression impossible. The amount of compression depends on the type of file. Word processing files can generally be compressed to less than half their original size. Graphics files can often be compressed even more than word processing files.

Select *ASCII encode after encrypting* to force Entrust to use an ASCII file format when encrypting and/or signing files. If you do not select this option, Entrust will use a binary format. One advantage of using the binary format is that the resulting size of the protected file is about 30% smaller than if you use the ASCII file format. Also, it takes less time to process files in binary format than it does to process files in ASCII file format. However, the ASCII option is mandatory if you plan to transfer the protected file using an electronic file transfer mechanism like ASCII-FTP or certain electronic mail systems that can only handle ASCII file formats.

Once your file is protected, its filename will receive the suffix specified in the *Output file extension* field. The default suffix is *ent*. You can change the output file suffix by entering a different one. It is recommended that you use

the default *ent* suffix to achieve consistency among Client users across all supported platforms. Using the default also makes it easier to find protected files. For example, if you protect a file called *report7.doc*, the filename of the protected file is *report7.doc.ent*.

CAST and DES are two encryption methods available to the Client to protect your files. Typically the decision on which to use is a policy adopted by your company or group with guidance from your Entrust Administrator.

7. Click the *Save as defaults* button to save the currently selected options in the *Entrust Options* dialog. The next time you encrypt and/or sign files, these options will be used unless you change them again.

If you change the default settings in this dialog and do not click the *Save as defaults* button, your changes will only apply to the current encrypt and/or sign operation and the next time you encrypt and/or sign files, the default settings will be used.

Note that if you use a recipients list, the options you save will be overridden by the options saved with the recipient list.

Now you are ready to encrypt and/or sign the selected files.

Encrypting and signing files

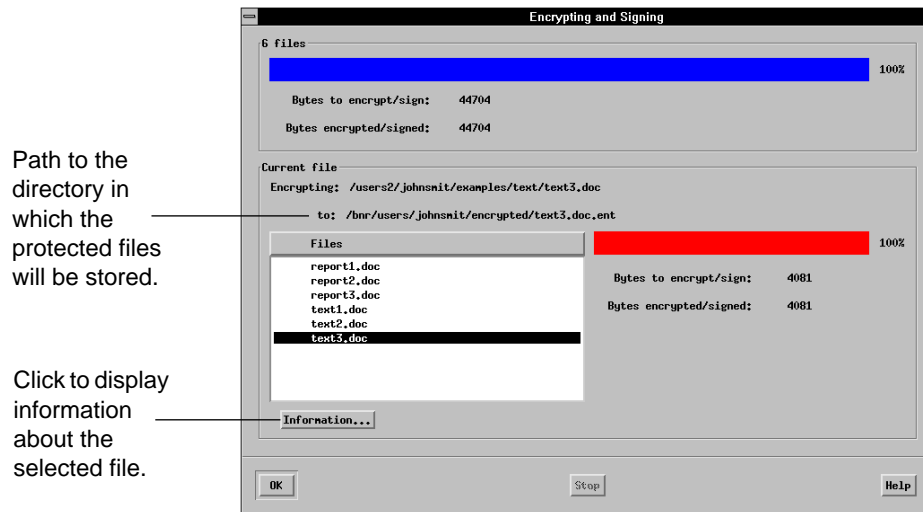
Once you have selected files to be protected, recipients (if applicable), and options, you are ready to encrypt and/or sign the selected files.

This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to “Selecting files to encrypt and sign” on page 48.

To encrypt and sign files, proceed as follows:

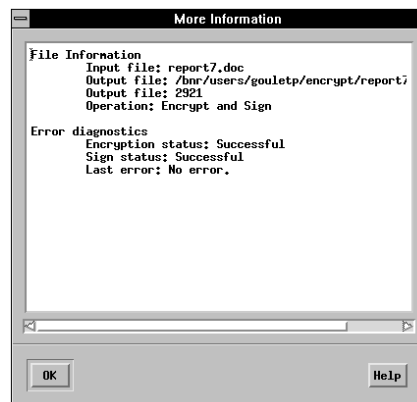
1. Click *OK* in the *Encrypt and Sign* dialog.

The *Encrypting and Signing* dialog appears and the files are encrypted and/or signed.



2. To display information about the files you just protected, select a file and click *Information...*

The *More Information* dialog appears displaying information about the protected file you selected.



3. Click *OK* to leave the *More Information* dialog.

The *Encrypting and Signing* dialog reappears.

4. Click *OK* to leave the *Encrypting and Signing* dialog.

The *Entrust* main window reappears.

The files you selected are now securely protected, and are stored in the directory you specified. If you look in that directory, you will notice that the files you protected have an *ent* filename extension; for example, if you protected a file called *report7.doc*, the filename of the protected file is *report7.doc.ent*.

You can now give the protected files to your chosen recipients. No one other than the chosen recipients and you will be able to decrypt the files.

You will notice a slight increase in the size of files after you encrypt and/or sign them. The size of a protected file depends on whether the file is only encrypted, only signed, or both encrypted and signed. The size of the protected file increases slightly for each recipient you include. Use of the *Compress before encrypting* and *ASCII encode after encrypting* options also affects the size of protected files.

ATTENTION

It is critical that you do not make changes to protected files. Even the slightest change to the files will cause corruption and make it impossible to decrypt and verify them at a later time.

Deleting files so that they are unrecoverable

You can use the *Secure Delete* function to securely delete files in such a way that the files are completely unrecoverable using any file-recovery utility. This prevents anyone from searching your hard disk to recover files deleted through the standard file system provided with your operating system.

Secure Delete uses a proprietary algorithm to ensure that the files you securely delete are completely overwritten on disk several times with random data.

ATTENTION

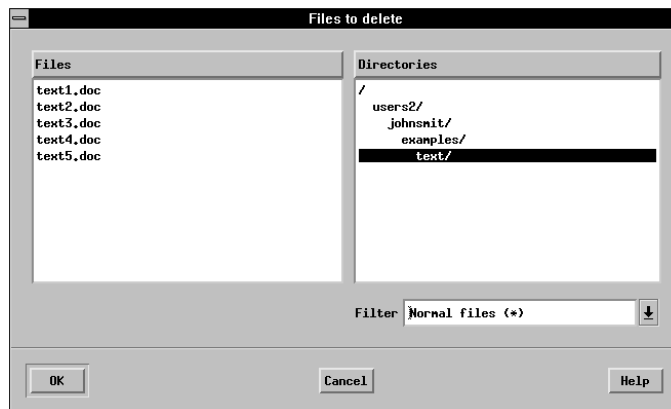
Use *Secure Delete* cautiously. Once files are securely deleted, they are gone forever. Remember that *Secure Delete* can only delete the files that you specify; therefore, remember to specify all copies of the files you want to delete.

Proceed as follows:

1. Click the *Secure Delete* icon in the *Entrust* main window.



The *Files to delete* dialog appears.

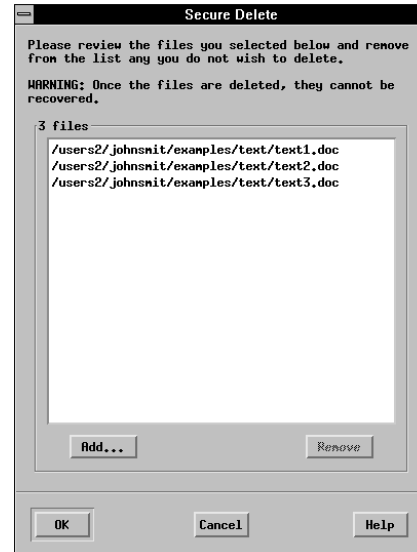


2. Locate the files you want to securely delete. If necessary, change directory or drive.

To change directory, click a directory name in the *Directories* list within the *Files to delete* dialog. Traverse branches as you would normally do in UNIX.

3. Select a single file you want to securely delete by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

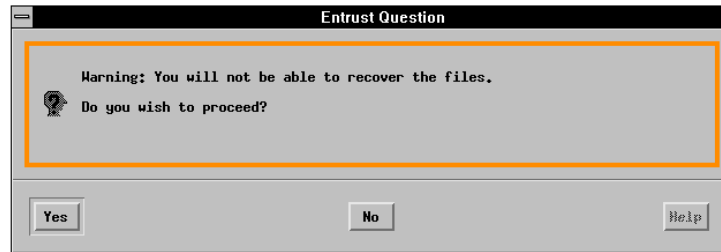
The *Secure Delete* dialog appears displaying the names of the files you selected.



4. You may still select more files to securely delete. Proceed as follows:
 - a. Click *Add...* in the *Secure Delete* dialog.
The *Files to delete* dialog reappears.
 - b. Navigate to the directory that contains the files you want to securely delete.
 - c. Select a single file you want to securely delete by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.
The *Secure Delete* dialog reappears.
 - d. Repeat steps 4.a. to 4.c. until you have selected all the files you require. You can select files from more than one directory.

5. Carefully verify the list of files you selected. You can remove files from the list in the *Secure Delete* dialog by selecting them and then clicking *Remove*.
6. Once you are certain you want to securely delete all the files in the list, click *OK* in the *Secure Delete* dialog.

The following reminder appears.



7. Click *Yes* if you are certain you want to securely delete the files.
If you click *No*, the *Secure Delete* dialog reappears.
Once the files are the deleted, the *Entrust* main window appears.

Decrypting and verifying protected files

A protected file is a file that is encrypted, signed, or both. If a file is encrypted, you will not be able to view its contents until it is decrypted. To decrypt a file means to restore it to the state it was in just prior to being encrypted.

To verify a digital signature means to check who signed the file and to ensure the file has not been modified since it was signed. A valid digital signature is a guarantee that the file has not been altered.

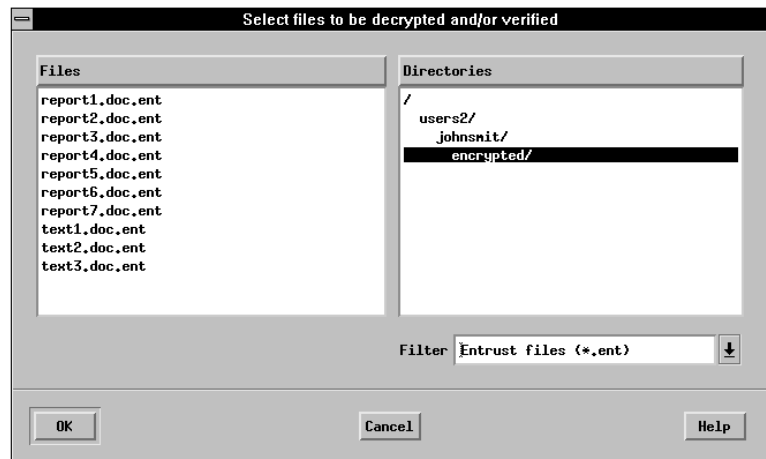
You do not have to specify whether you want to decrypt, verify, or both decrypt and verify a protected file. The Client automatically performs the appropriate operation(s) once it detects whether a protected file is encrypted, signed, or both encrypted and signed.

To decrypt and verify protected files, proceed as follows:

1. Click the *Decrypt and Verify* icon in the *Entrust* main window.



The *Select files to be decrypted and/or verified* dialog appears.

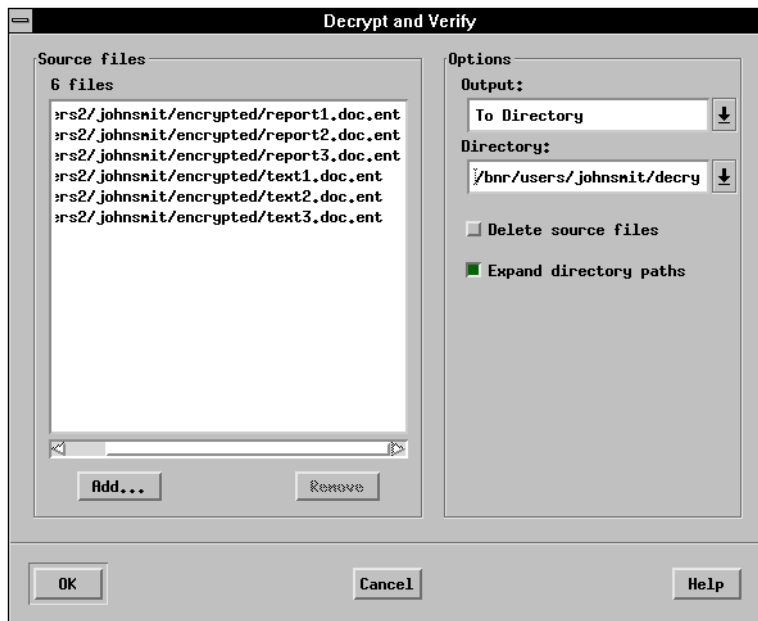


2. Navigate to the directory that contains the files you want to decrypt and verify.

To change directory, click a directory name in the *Directories* list within the *Select files to be decrypted and/or verified* dialog. Traverse branches as you would normally do in UNIX.

3. Select a single file you want to decrypt and verify by double-clicking it. Alternatively, you can select several files by clicking the filenames while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

The *Decrypt and Verify* dialog appears displaying the names of the files you selected.



4. You may select more files to unprotect. Proceed as follows:

- a. Click *Add...* in the *Source files* section of the *Decrypt and Verify* dialog.

The *Select files to be decrypted and/or verified* dialog reappears.

- b. Navigate to the directory that contains the files you want to decrypt and verify.

To change directory, click a directory name in the *Directories* list within the *Select files to be decrypted and/or verified* dialog. Traverse branches as you would normally do in UNIX.

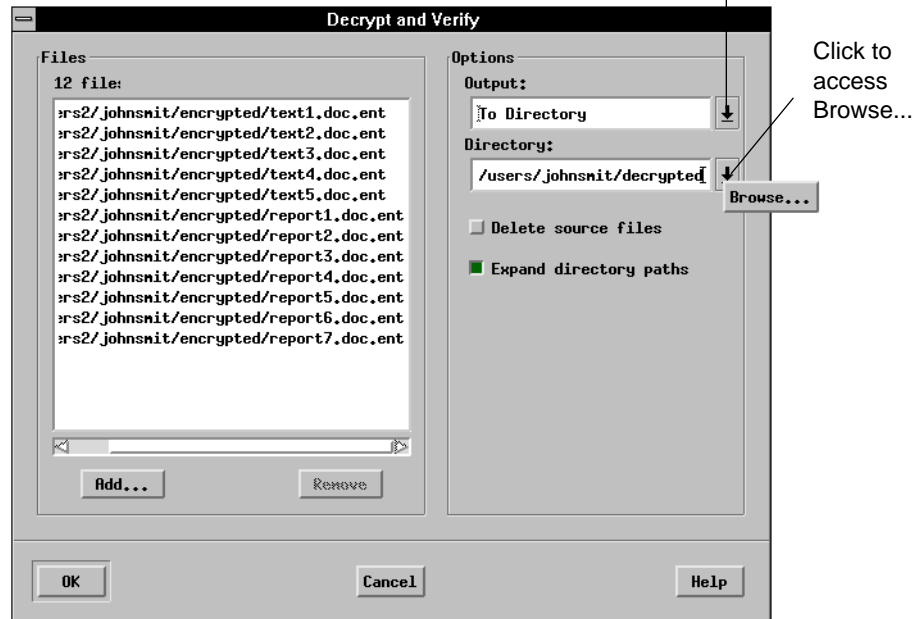
- c. Select a single file you want to decrypt and verify by double-clicking it. Alternatively, you can select several files by clicking each one while holding down either the *Shift* or *Ctrl* key and then clicking *OK*.

The *Decrypt and Verify* dialog reappears displaying the files you selected.

- d. Repeat steps 4.a. to 4.c. until you have selected all the files you require. You can select files from more than one directory.

5. Notice the *Output* field.

Click to display all output options.



The *Output* field determines where the decrypted files will be stored. Valid settings are as follows:

- To Directory
- In Place
- No output (verify only)

Select *To Directory* to store the decrypted files in a directory specified by the *Directory* field.

When you unprotect a file, the Client stores the unprotected file in the directory that you specify in the *Directory* field. This directory selection remains in effect until you change it. The *Directory* field only appears if the *Output* field is set to *To Directory*. Note that the protected file is left intact.

Select *In Place* to store the unprotected files in the same directory as the protected files.

Select *No output (verify only)* to verify the digital signature of each protected file without writing the unprotected files to disk.

6. In the *Directory* field, enter the full path to the directory in which you want to store your decrypted files. If the directory does not already exist, you will be prompted to create it.

Alternatively, you can use *Browse...* to locate and select an existing directory in which to store your decrypted files.

The *Directory* field and *Browse...* are only available when the *Output* field is set to *To Directory*; however, the directory you specify in the *Directory* field will remain in effect until you change it again.

7. Notice the *Delete source files* selection box in the *Decrypt and Verify* dialog.

Select *Delete source files* to automatically delete the original files after they are unprotected. If you do not select this option, the original, protected files will remain intact after a copy of each file is decrypted.

8. Notice the *Expand directory paths* selection box.

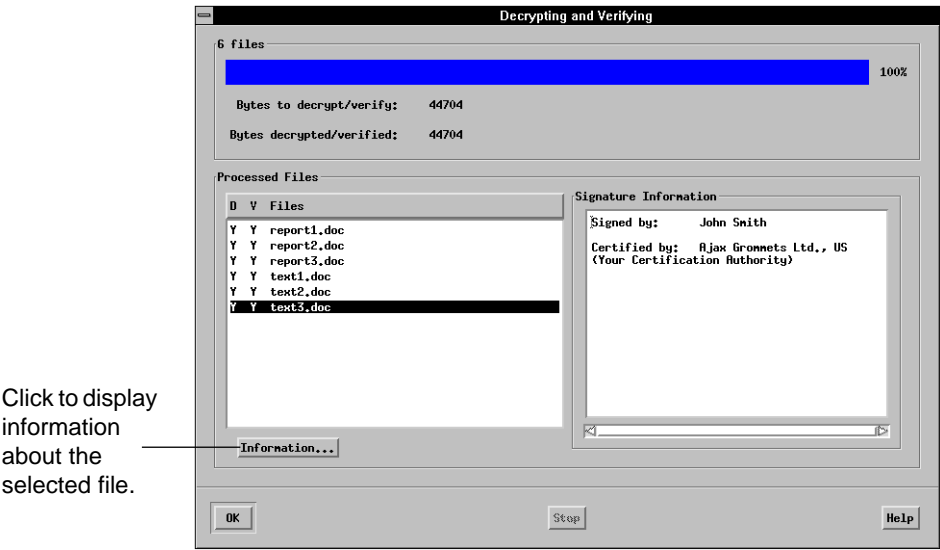
This option only applies if you are decrypting a protected archive file that contains other directories which in turn contain protected files. Such an archive can only have been created by the Windows version of the Client.

Select *Expand directory paths* to preserve the directory structure of the archive file you are unprotecting.

Deselect *Expand directory paths* to store all unprotected files in the same directory (specified by the *Output* field) after they are unprotected. If there are files with the same names, you will be prompted to rename them.

9. Once you have selected the files you want to unprotect, you are ready to begin the decryption and verification process. Click *OK* in the *Decrypt and Verify* dialog.

The *Decrypting and Verifying* dialog appears.



The capital Y (yes) in the column headed by the capital D (decrypt) means the file was decrypted. If a blank appears instead, it means the file was not decrypted because it was not previously encrypted. The capital Y in the column headed by the capital V (verify) means that the file was signed and that the signature was verified. If a blank appears instead, it means the file was not verified because it was not previously signed. If a blank appears in both columns, it means the file was never processed by Entrust.

D	V	Files
Y	Y	report1.doc.ent
Y		report2.doc.ent
	Y	report3.doc.ent
Y	Y	report4.doc.ent
Y		report5.doc.ent
Y		report6.doc.ent

Note: If a capital N or a ? appears instead of a Y or a blank in either column, refer to “Symbols that indicate problems with protected files” on page 82 for an explanation.

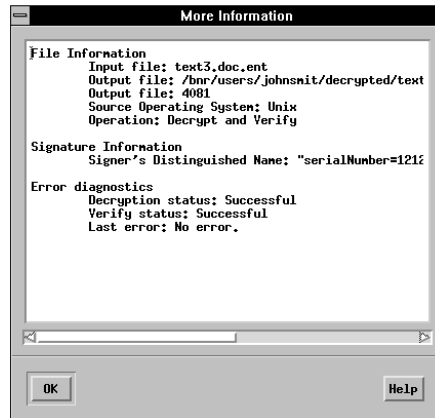
D	V	Files
Y		encryptonly.ent
N		encryptonlyWithTampering.ent
Y	Y	signandencrypt.ent
N	N	signandencryptWithTampering.ent
Y		signonly.ent

10. Notice the *Signature Information* section of the *Decrypting and Verifying* dialog. It shows the name of the person who signed the currently selected file and the name of the Certification Authority that certified the signature.

The Certification Authority comprises one or more people who are responsible for security policy decisions in the organization.

11. To display information about the files you just unprotected, select one of the files and click *Information...*

The *More Information* dialog appears displaying information about the unprotected file you selected.



12. Click *OK* to leave the *More Information* dialog.

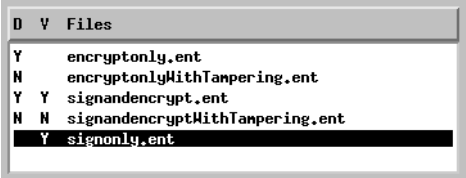
The *Decrypting and Verifying* dialog reappears.

13. Click *OK* to leave the *Decrypting and Verifying* dialog.

Your files are now unprotected. You can open, move, and rename these files.

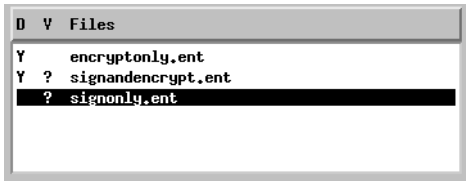
Symbols that indicate problems with protected files

If a capital N appears in the column headed by the capital D, it means that the file could not be decrypted. If a capital N appears in the column headed by the capital V, it means that the signature associated with the file could not be verified. The reason the file could not be decrypted and/or verified may be that someone tampered with the protected file after it was encrypted and/or signed. You should ask the person who gave you the protected file to give you a new copy to decrypt.



D	V	Files
Y		encryptonly.ent
N		encryptonlyWithTampering.ent
Y	Y	signandencrypt.ent
N	N	signandencryptWithTampering.ent
Y		signonly.ent

If a ? appears in the column headed by the capital V, it means that the file was signed but that you should not necessarily trust the signature.



D	V	Files
Y		encryptonly.ent
Y	?	signandencrypt.ent
?		signonly.ent

There are two possible reasons why you should not necessarily trust the signature.

One reason is that the signing key used to sign the file is no longer valid. Ask the person who gave you the file to sign it again and to give you a new copy. Verify the new signed file to ensure the signature is valid.

The other reason you should not trust the signature is that you do not have a network connection; therefore, Entrust could not update your Entrust signature verification information. Without access to this information, Entrust cannot verify that the signature used to sign the file is valid. Once you have regained access to the network, you can verify the signature with the assurance that the signature is valid. For more information about this situation, refer to “Cannot update your Entrust signature verification information” on page 127.

Exchanging protected files with users in different domains

There may be times when you want to exchange protected files with people who use Entrust in different CA security domains.

Within the context of Entrust, a CA security domain is a group of people who use Entrust under the same software license and have been certified by the same Certification Authority (CA). Typically, these users have something in common (for example, they all work in the same company or they work on the same project).

If you want to exchange protected files with someone who uses the Client in a domain that is different from yours, you need to obtain that user's Entrust address and associated validation string. Refer to "Entrust address" and "Validation string" on this page for more information about these terms.

As people give you copies of their Entrust addresses and validation strings, you should import the address information into your address book. You will not be able to exchange protected files with people who use Entrust in a domain that is different from yours unless you import their address information first. Refer to "Address book" on page 84 for more information about address books.

Entrust address

An Entrust address provides the necessary information to ensure that files encrypted and signed by someone using Entrust in one domain can be decrypted and verified by someone using Entrust in other domains.

An Entrust address is stored in a *key* file and all users can export their own *key* files for users in other security domains to import. The filename comprises your Client username with a *key* filename extension (for example, *johnsmit.key*). For information about exporting your Entrust address, refer to "Exporting your personal Entrust address" on page 91.

Validation string

A validation string is a string of alphanumeric characters (for example, 7CN4-YL5D-HP7V) that is automatically generated by the Client when you export your address. Each Entrust address has a unique validation string which is associated with the *key* file. Use the validation string to confirm that the address someone gives you in a *key* file has not been tampered with since it was created.

When you export your own Entrust address in a *key* file, the associated validation string appears in a dialog. Whenever you give someone the *key* file, also tell them the validation string. Give people the *key* file and the validation string separately (unless you give them this information in person). Moreover, when you give someone the validation string, you must use a method that guarantees its authenticity. For example, you can send people the *key* file as an e-mail attachment or stored on a floppy diskette, and tell them the validation string in person or by telephone. Note that if you use the telephone, the validation string can only be considered authentic if the person to whom you give the validation string can recognize your voice. If the person cannot recognize your voice, then another method must be used (for example, registered mail or a meeting in person).

Note: It is best to export a new *key* file whenever you want to give your Entrust address to someone.

When someone gives you a *key* file, ask the person for the associated validation string. Ensure the validation string is authentic as described above. When you import that *key* file into your address book, the validation string is displayed in a dialog. Compare that validation string with the one you were given. If they match, the *key* file is genuine and can be trusted. If they do not match, ask the person to give you a new copy of the *key* file and the new associated validation string.

Address book

An address book contains the Entrust addresses of people in other domains with whom you plan to exchange protected files. The filename of the file that contains your address book comprises your Client username with a *pab* (personal address book) filename extension (for example, *johnsmit.pab*).

Creating and accessing your address book

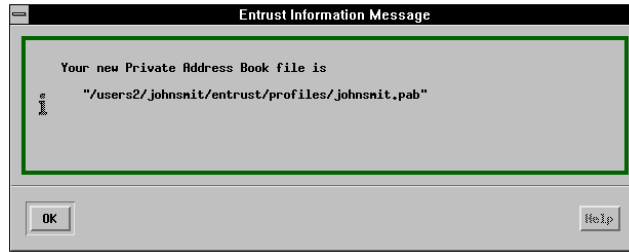
You will need to create an address book if you intend to exchange protected files with people outside of your security domain.

To create or access your address book, proceed as follows:

1. Choose *Address Book Services...* from the *File* menu.

Your address book appears immediately if you previously created it.

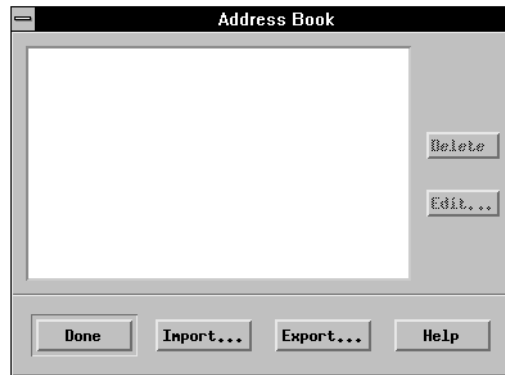
If this is the very first time you access *Address Book Services*, the Client displays the following message.



Note: If you previously created an address book and subsequently moved it, the Client will not be able to access it and you will be forced to create a new one. If you move your address book file (*pab*) to a different directory after you create it, you will also need to move your profile to the same directory. Similarly, if you need to move your profile to a different directory, move your address book file to the same directory as your profile.

2. Click *OK* in the message dialog shown above to create your address book.

The *Address Book* dialog appears.



You can now build your address book by importing the addresses of people with whom you want to exchange protected files.

You can also export your personal Entrust address as explained in "Exporting your personal Entrust address" on page 91.

Building your address book

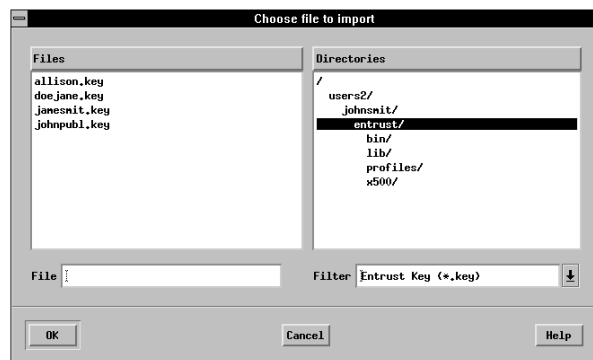
Building your address book involves importing the addresses of people in other Entrust security domains with whom you plan to exchange protected files. You can add and remove people from your address book at any time. Note that when you look at your address book, you will see the names of people who use Entrust outside your CA security domain; you will not see their addresses. The actual address information is stored in your address book (*pab*) file and can only be accessed by the Client.

This procedure assumes you already accessed your address book. If you have not yet accessed your address book, refer to “Creating and accessing your address book” on page 84.

To import addresses of other Entrust users into your address book, proceed as follows:

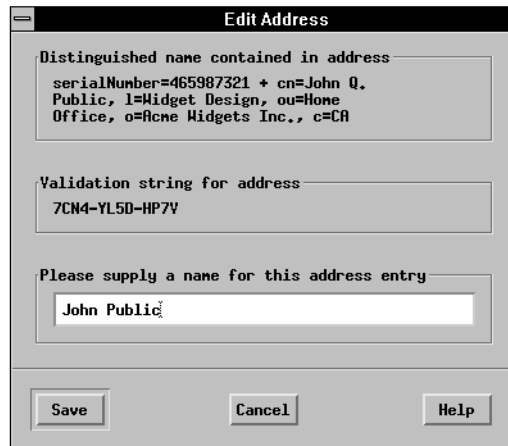
1. From the *Address Book* dialog, click *Import...*

The *Choose file to import* dialog appears.



2. From this dialog, locate the *key* file that contains the address you want to add to your address book (for example, *johnpubl.key*). If necessary, change directory.
3. Once you have found the *key* file, select it and click *OK* in the *Choose file to import* dialog.

The *Edit Address* dialog appears. This dialog contains the validation string associated with the address you are adding to your address book.



4. Check the validation string (for example, 7CN4-YL5D-HP7V) in the *Edit Address* dialog. It must match exactly the validation string the person gave you. The hyphens are optional.

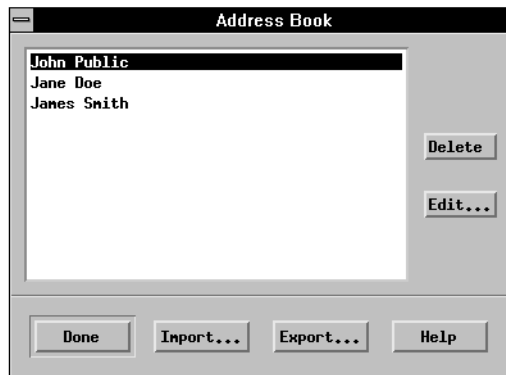
If the validation string does not match, the *key* file may have been damaged or maliciously changed since it was created. Ask the person who gave you the *key* file to give you a new *key* file and the associated validation string.

If the validation string matches, continue at step 5.

5. Click *Save*.

The *Address Book* dialog reappears and the name of the person you just added appears in the address book.

6. Repeat the procedure for each address you want to add to your address book.



7. Click *Done* once you have finished adding people to your address book.

Now you can protect files for anyone listed in your address book.

Whenever you need to exchange protected files with an Entrust user outside your domain, you can retrieve the user's name from your address book when selecting recipients for your encrypted file. For information about selecting recipients from your address book, refer to "Selecting recipients by name in personal address book" on page 57.

Changing the contents of your address book

You can make the following changes to your address book:

- Delete the names of people from your address book.
- Change the names of people who are already in your address book.
- Re-import the addresses of people who are already in your address book.

Deleting people from your address book

To delete a person from your address book, proceed as follows:

1. From the *Address Book* dialog, select the person you want to remove.
2. Click *Delete* to delete the person.
A confirmation dialog appears.
3. Click *OK* in the confirmation dialog.

The *Address Book* dialog reappears.


Changing the names of people who are already in your address book

You can change the name of a person who is already listed in your address book. You might do this if you want to add more information to the name (for example, the person's company name). This change has no effect on the person's Entrust address; it only changes the way the person's name appears in your address book.

To change the name of a person who is already listed in your address book, proceed as follows:

1. From the *Address Book* dialog, select the person whose name you want to change.
2. Click *Edit...*

The *Edit Address* dialog appears. This dialog contains information about the person whose name you are changing.

The screenshot shows a dialog box titled "Edit Address". It contains three text fields. The first field is labeled "Distinguished name contained in address" and contains the text "serialNumber=465987321 + cn=John Q. Public, l=Midget Design, ou=Home Office, o=Acme Widgets Inc., c=CA". The second field is labeled "Validation string for address" and contains the text "7CN4-YL5D-HP7Y". The third field is labeled "Please supply a name for this address entry" and contains the text "John Public - Mgr at Main Office Equipment". At the bottom of the dialog are three buttons: "Save", "Cancel", and "Help".

3. Enter a unique name for the person in the field at the bottom of the dialog.
This is the name that will appear in your address book.
4. Click *Save*.
The *Address Book* dialog reappears.

Re-importing the addresses of people into your address book

If people whose names already appear in your address book change their Entrust addresses (for example, if they move from one company to another), you will need to delete their old addresses from your address book and re-import each person's new address.

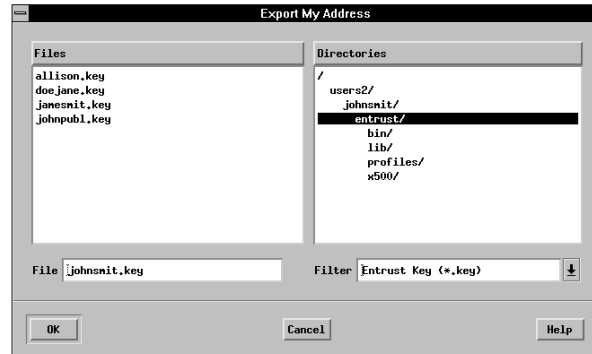
If people whose names already appear in your address book ever recover their Client username, (as explained in "Recovering your Entrust/Client username" on page 112) those people should give you new *key* files (and associated validation strings) which you should import into your address book.

Exporting your personal Entrust address

To allow other Entrust users outside your security domain to send protected files to you, you must give them your Entrust address. This address must be placed in a *key* file as follows:

1. From the *Address Book* dialog, click *Export...*

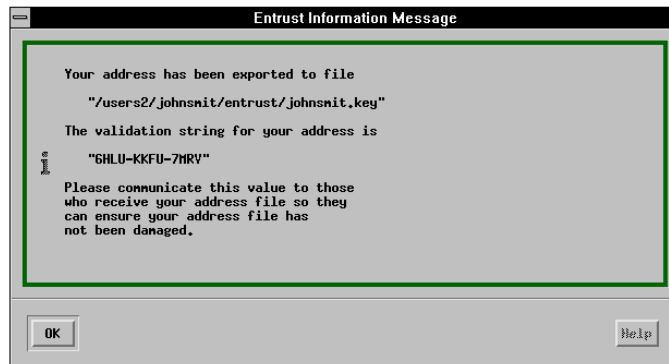
The *Export My Address* dialog appears displaying the name of a file called *Client_username.key* (for example, *johnsmit.key*).



2. If you want to use the default filename displayed in the *File* field for your key file, click *OK*.

Alternatively, you can enter a different filename and click *OK*. You can also select a different directory in which to store the file.

A dialog appears explaining that your address has been created. The dialog also displays the validation string (for example, 6HLU-KKFU-7MRV) associated with your address. Take note of the validation string. When you give your *key* file to Entrust users in other CA security domains, you must tell them the validation string.



3. Click *OK*.

The *Address Book* dialog reappears.

The *key* file containing your Entrust address is created. You can give this file to Entrust users in other CA security domains so they can protect files for you. Remember to tell these users the validation string associated with your address. You should give people the *key* file and the validation string separately (unless you give them this information in person).

For example, you can send people the *key* file as an e-mail attachment or stored on a floppy diskette, and tell them the validation string in person or by telephone. When you give someone the validation string, you must use a method that guarantees its authenticity. For example, if you tell them the validation string by telephone, the validation string can only be considered authentic if the person to whom you give the validation string can recognize your voice. If the person cannot recognize your voice, then another method must be used (for example, registered mail or a meeting in person).

Using saved lists of recipients

An Entrust/Client recipient list is a set of recipients and options for encrypting and signing that you select and store under a *recipient list* name. Instead of having to specify each recipient and option every time you want to protect files, you can specify the name of a recipient list. You control who is part of a recipient list and you can create more than one recipient list. For example, you could create one recipient list for each project you work on. Note that a recipient can be a member of more than one recipient list.

For example, you may find that you always use file compression and ASCII encoding when you protect files to be sent to a group of users via e-mail but that you use other options when you frequently protect files for a different group of users. For those two scenarios, you could create two separate recipient lists that would make protecting files for these groups of users very simple.

A recipient list can include recipients who are part of your CA security domain and Entrust users in other domains. To include recipients from other domains, you first need to import their Entrust addresses. See “Exchanging protected files with users in different domains” on page 83 for more information about including recipients from other domains.

An important feature of recipient lists is that they can be shared with other Client users in your domain. For example, if you and your colleagues use some of the same recipient lists on a regular basis, you can share them instead of maintaining your own copies of the same recipient lists. You can share your own recipient lists by exporting them, or you can share other users’ recipient lists by importing them. Refer to “Sharing recipient lists” on page 101.

The recipient lists are stored in a separate file. The filename is the same as your username. An *erl* filename extension is automatically added to the filename of the recipient list file (for example, *johnsmit.erl*).

Recipient list management functions are as follows:

- create
- duplicate
- change
- delete
- share

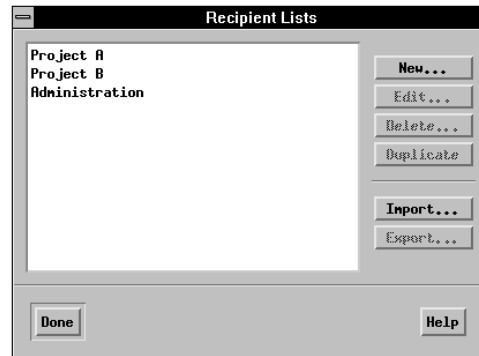
Accessing recipient list management functions

Proceed as follows to access recipient list management functions:

1. Click the *Recipient Lists* icon in the *Entrust* main window.



The *Recipient Lists* dialog appears. Note that in this example there are some existing recipient lists.



2. From the *Recipient Lists* dialog you can:
 - create new recipient lists (see “Creating a new recipient list” on page 95)
 - change existing recipient lists (see “Changing an existing recipient list” on page 98)
 - delete existing recipient lists (see “Deleting an existing recipient list” on page 100)
 - share your recipient lists (see “Sharing your recipient lists with other users” on page 101)
 - import shared recipient lists (see “Sharing other users’ recipient lists” on page 103)

Creating a new recipient list

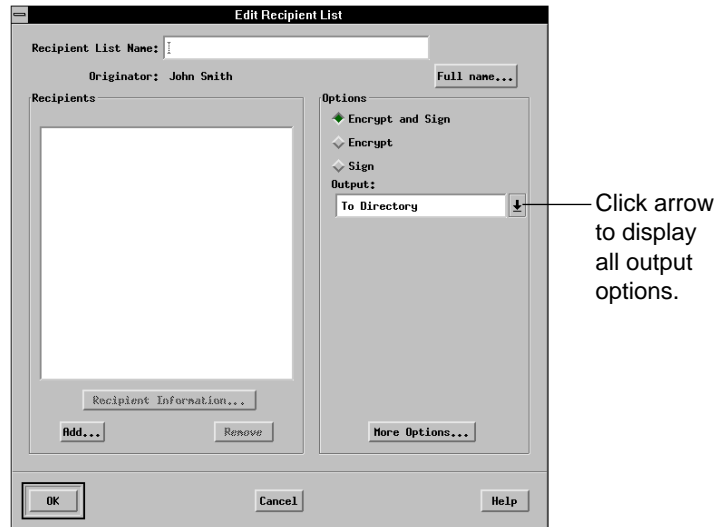
This procedure assumes that the *Recipient Lists* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 94.

Note: If you want to create a new recipient list that is based on an existing recipient list, duplicate an existing recipient list then make changes to the new (duplicate) recipient list. Refer to “Changing an existing recipient list” on page 98 for information about making changes to a recipient list.

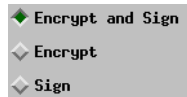
To create a new recipient list, proceed as follows:

1. Click *New...* in the *Recipient Lists* dialog.

The *Edit Recipient List* dialog appears.



2. Enter the name of your new recipient list in the *Recipient List Name* field in the *Edit Recipient List* dialog.
3. Select one of the following options:



Select *Encrypt and Sign* to encrypt and sign the selected files.

Select *Encrypt* to encrypt the selected files without including your signature.

Select *Sign* to include your signature with the selected files. The files will not be encrypted. You would select this option if you were sending out information that is well known (hence it does not need to be encrypted), but you want your recipients to be assured that the information originated from you and that it has not been tampered with since you signed it.

4. Notice the *Output* field.

The *Output* field determines where the protected files will be stored. Valid settings are as follows:

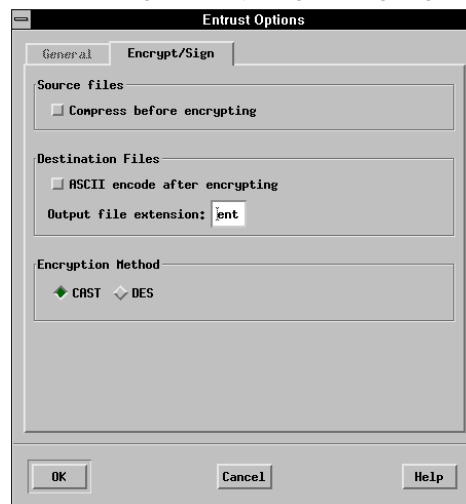
- To Directory
- In Place

Select *To Directory* to store the protected files in a directory specified by the *Directory* field in the *Encrypt and Sign* dialog. When you protect a file, the Client stores the protected file in the directory that you specify in the *Directory* field. This directory selection remains in effect until you change it. The *Directory* field in the *Encrypt and Sign* dialog only appears if the *Output* field is set to *To Directory*. Note that the original, unprotected file is left intact.

Select *In Place* to store the protected files in the same directories as the original unprotected files. This option will also work if you select files from different directories.

5. Click *More Options...* in the *Edit Recipient List* dialog.

The *Entrust Options* dialog for encrypting and signing appears.



Encrypt and sign options you can select are as follows:

- Compress before encrypting
- ASCII encode after encrypting
- Output file extension
- Encryption Method

The options you choose in the *Entrust Options* dialog will be automatically selected whenever you use the recipient list in the *Encrypt and Sign* dialog. For more information about the options, refer to “Selecting encrypting and signing options” on page 66.

Click *OK* to leave the *Entrust Options* dialog once you have selected the appropriate options for the recipient list.

6. Click *Add...* to specify the recipients to be stored as part of the recipient list.

The rest of the procedure for creating a new recipient list depends on whether you want to add recipients by

- searching for names of people (see “Selecting recipients by name” on page 52)
- selecting names of people who are members of one of your existing recipient lists (“Selecting an existing recipient list from the Recipients dialog” on page 63)
- selecting names of people whom you previously imported into your address book (“Selecting recipients by name in personal address book” on page 57)

You can add names to the recipient list by combining any of these three methods. You can also delete recipients from a recipient list.

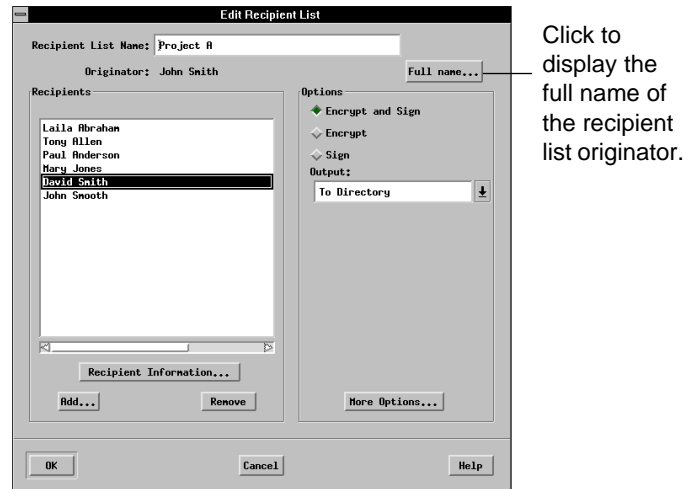
Changing an existing recipient list

This procedure assumes that the *Recipient Lists* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 94.

To change an existing recipient list, proceed as follows:

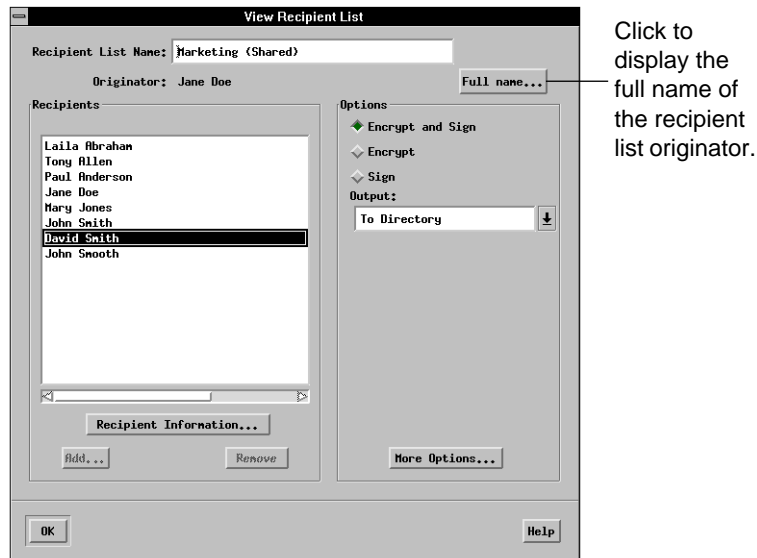
1. Select the recipient list name from the *Recipient Lists* dialog and click *Edit...* Alternatively, you can double-click the recipient list name.

The *Edit Recipient List* dialog appears. The name of the recipient list you selected appears in the *Recipient List Name* field and the recipients that are currently members of the recipient list appear in the *Recipients* section of the *Edit Recipient List* dialog.



If the *View Recipient List* dialog appears instead of the *Edit Recipient List* dialog, it means you selected a shared recipient list. Shared recipient lists cannot be modified directly. Only the originators of shared recipient lists can make changes to shared recipient lists and they can only change the original recipient lists; they cannot edit the shared version of the recipient

lists. Refer to “Sharing recipient lists” on page 101 for information about shared recipient lists.



2. You can click *Full name...* to display the name of the person who created the shared recipient list. If you need changes to the shared recipient list, you can ask the originator to make them.
3. You can display information about a recipient by selecting the recipient's name and clicking *Recipient Information...*
4. Select options to be stored with your recipient list. Refer to step 3. in “Creating a new recipient list” on page 95 for information about selecting options in a recipient list.

If you attempt to make changes to a recipient list and the following message appears, it is because you selected a shared recipient list.



The rest of the procedure for changing an existing recipient list depends on whether you want to add recipients by

- searching for names of people (see “Selecting recipients by name” on page 52)

- selecting names of people who are members of one of your existing recipient lists (“Selecting an existing recipient list from the Recipients dialog” on page 63)
- selecting names of people whom you previously imported into your address book (“Selecting recipients by name in personal address book” on page 57)

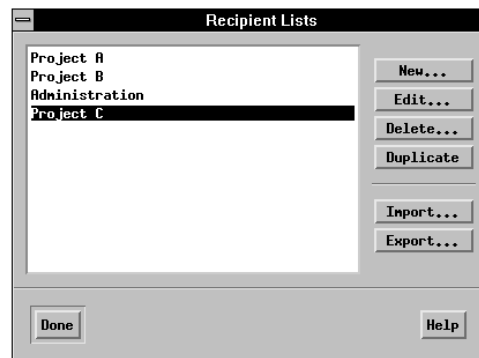
You can add names to the recipient list by combining any of these three methods. You can also delete recipients from a recipient list.

Deleting an existing recipient list

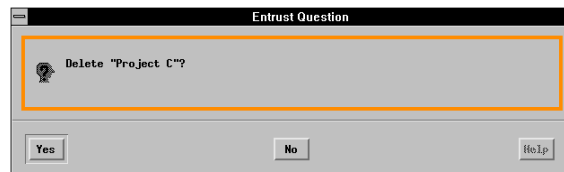
This section assumes the *Recipient Lists* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 94.

To delete an existing recipient list, proceed as follows:

1. Select the recipient list name you want to delete from the *Recipient Lists* dialog and click *Delete...*



A confirmation dialog similar to the following appears.



2. Click Yes.

The *Recipient Lists* dialog reappears.

Your recipient list is deleted.

Sharing recipient lists

An important feature of recipient lists is that you can share them with other Client users in your CA security domain. For example, if you and your colleagues use some of the same recipient lists on a regular basis, you can share them instead of maintaining your own copies of the same recipient lists.

You can share some of your own recipient lists with others; similarly, you can use a recipient list that was created by someone else.

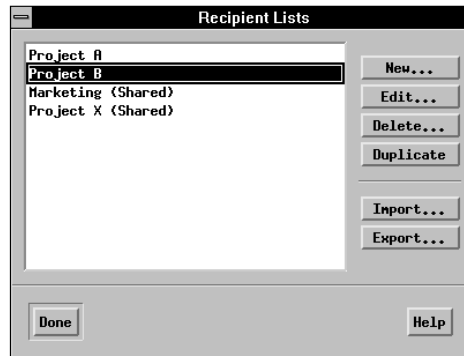
Sharing your recipient lists with other users

This section assumes the *Recipient Lists* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 94.

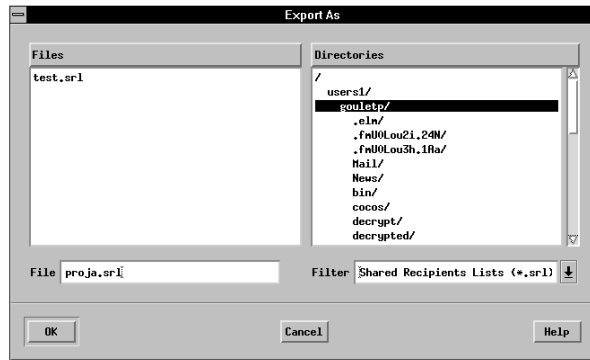
To share your recipient lists, proceed as follows:

1. Select the recipient list name you want to share from the *Recipient Lists* dialog and click *Export...*

Note: If the recipient list you select contains recipients from your personal address book, these recipients will be rejected when people try to share the recipient list (unless those people have also imported the Entrust addresses of those recipients into their own personal address books).

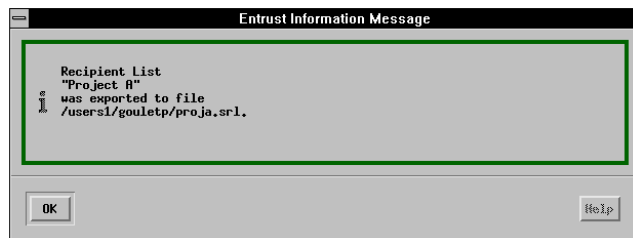


The *Export As* dialog appears.



2. In the *File* field, enter a filename for the file in which you want to store your shared recipient list. Notice that the default filename extension is automatically *srl*. This extension is mandatory and cannot be changed.
3. Choose a directory in which you want to store your shared recipient list file.
4. Click *OK* in the *Export As* dialog.

A message similar to the following appears.



5. Click *OK*.

The *Recipient Lists* dialog reappears.

Your recipient list has been exported. Ensure this file is stored in a directory to which others have access so they can use this recipient list when selecting recipients or when creating or editing other recipient lists.

ATTENTION

Shared recipient lists cannot be modified by anyone including the originator. Therefore you should keep a copy of the recipient list that you exported in case you need to make changes later. If you make changes to the recipient list, you will need to re-export the recipient list.

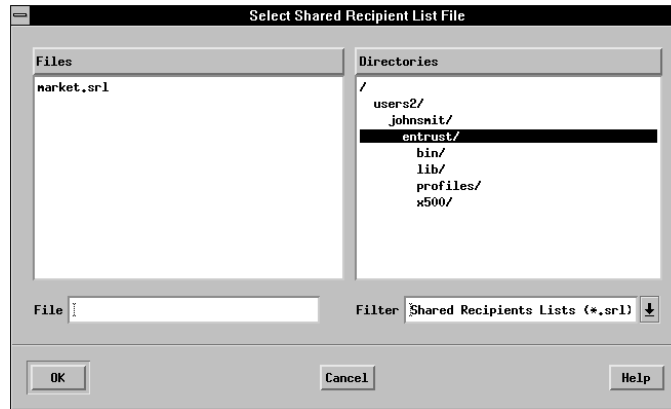
Sharing other users' recipient lists

This section assumes the *Recipient Lists* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 94.

To access recipient lists that were created by other users and that have been designated as shared recipient lists, proceed as follows:

1. Click *Import...* in the *Recipient Lists* dialog.

The *Select Shared Recipient List File* dialog appears.



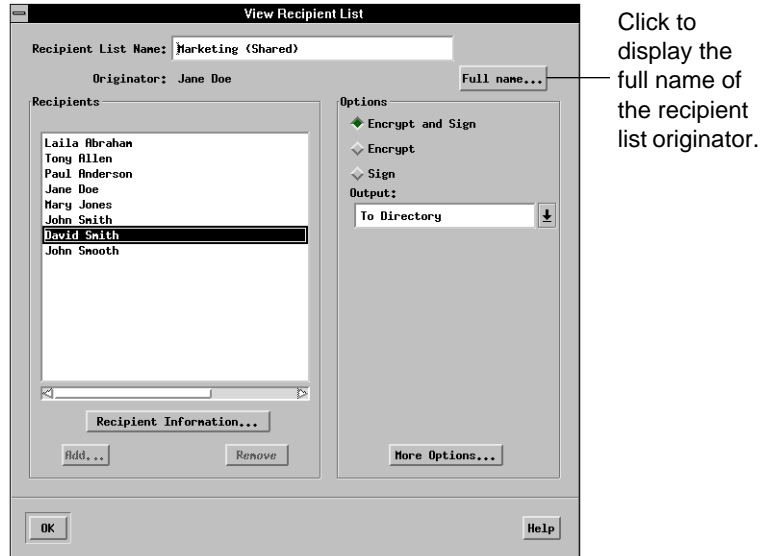
2. From this dialog, locate and select the *srl* file that contains the recipient list you want to use (for example, *Customers.srl*). If necessary, change directory.
3. Click *OK* in the *Select Shared Recipient List File* dialog.

The following dialog appears.



4. Click *OK*.

The *View Recipient List* dialog appears.



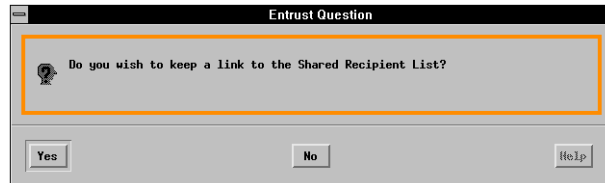
5. Review the recipient list and decide if you want to keep it. You cannot make changes to a shared recipient list.

You can click *Full name...* to display the name of the person who created the shared recipient list. If you need changes to the shared recipient list, you can ask the originator to make them.

You can display information about a recipient by selecting the recipient's name and clicking *Recipient Information...*

6. Click *OK* in the *View Recipient List* dialog.

The following dialog appears.



7. Click *Yes* if you want to keep the recipient list as is. Otherwise, you can click *No* to exit without saving a link to the shared recipient list.

In either case, the *Recipient Lists* dialog reappears.

You can use a shared recipient list when selecting recipients or when creating or editing other recipient lists. Notice that the recipient lists you imported have the word *Shared* within parentheses in the *Recipient Lists* dialog. When you select a shared recipient list, the *Edit...* button in the *Recipient Lists* dialog changes to *View...* because shared recipient lists cannot be modified.

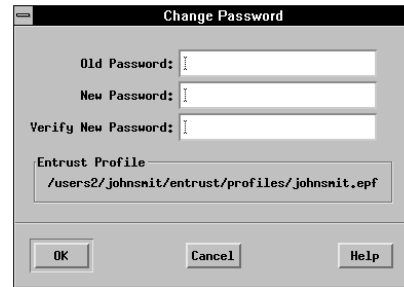
If the originator modifies and re-exports a shared recipient list that you have imported, you will be notified automatically that the recipient list has changed the next time you access it.

Changing your Entrust/Client password

To change your password, proceed as follows:

1. Choose *Change Password...* from the *File* menu.

The *Change Password* dialog appears.



2. Enter your current Client password in the *Old Password* field.
3. Tab to the *New Password* field and enter a password.

Your Client password must

- be at least eight characters long (however, as you make your password longer, it becomes significantly more difficult for an attacker to guess the password you select)
- contain at least one upper case letter
- contain at least one lower case letter
- not contain many occurrences of the same character
- not be the same as your Client username
- not contain a substring of your Client username

The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: \$, +, =, !, ~, ^ and &. A good password is one that is difficult to guess yet easy to remember (for example, H2OPIsNow! (water please, now!)). For more information about passwords, refer to "Appendix C: Entrust password security."

4. Tab to the *Verify New Password* field and enter the same password again.

The reason you need to enter your new password twice is to ensure that you typed exactly what you intended to type. The Client checks to ensure that you entered your new password exactly the same way both times.

If you write down your password, store it in a locked place to which only you have access.

5. Click *OK*.

Your password is changed.

Creating additional Entrust/Client usernames

There may be occasions when more than one Client username is required. To create a Client username, you will need a reference number (for example, 91480170) and an authorization code (for example, CMTJ-8VOR-VFNS). If you do not have this information already, contact your Entrust Administrator to obtain it. Your Administrator will tell you your reference number and authorization code in a confidential and secure manner.

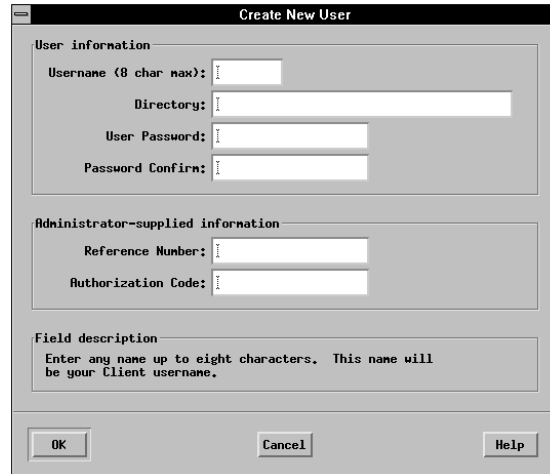
ATTENTION

Keep your reference number and authorization code confidential. Ensure you destroy them after you have created your Client username.

To create a Client username:

1. Select *Create New User...* from the *File* menu.

The *Create New User* dialog appears. Notice the *Field description* area at the bottom of the dialog. This area provides a brief description of the information you need to enter in each field of the dialog. Simply click in any field and the corresponding description will appear in the *Field description* area.



2. Enter a name in the *Username* field.

You can choose any name you like, but you are limited to eight characters (for example, *johnsmit*).

3. Tab to the *Directory* field and enter the name of the directory in which you want to store your profile. If the directory does not already exist, the Client will create it.
4. Tab to the *User Password* field and enter a password.

Your Client password must

- be at least eight characters long (however, as you make your password longer, it becomes significantly more difficult for an attacker to guess the password you select)
- contain at least one upper case letter
- contain at least one lower case letter
- not contain many occurrences of the same character
- not be the same as your Client username
- not contain a lengthy substring of your Client username

The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: \$, +, =, !, ~, ^ and &. A good password is one that is difficult to guess yet easy to remember (for example, H2OPlsNow! (water please, now!)). For more information about passwords, refer to "Appendix C: Entrust password security."

5. Tab to the *Password Confirm* field and enter the same password again.

The reason you need to enter your new password twice is to ensure you typed exactly what you intended to type. The Client checks to ensure that you entered your new password exactly the same way both times.

If you write down your password, store it in a locked place to which only you have access.

6. Tab to the *Reference Number* field and enter the reference number you obtained from your Administrator (for example, 91480170).
7. Tab to the *Authorization Code* field and enter the authorization code you obtained from your Administrator (for example, CMTJ-8VOR-VFNS). The hyphens are optional.
8. Click *OK*.

After a short period of time, the *Entrust Options* dialog appears if Entrust was able to create a new username. The *Entrust Options* dialog contains tabs that let you choose various types of options you want to change.



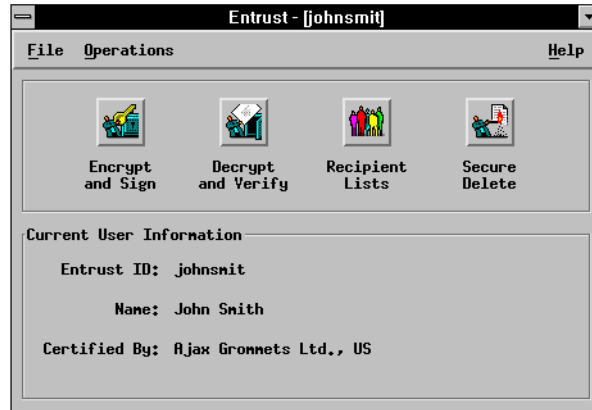
Note: If Entrust was unable to create a new username, try supplying the information again. Ensure that you enter the reference number and authorization code in exactly the same form as you received them from your Entrust Administrator. If you still cannot create a Client username, contact your Administrator.

9. Notice the *Logoff timeout* field in the *Entrust Options* dialog. This field specifies the length of time during which the Client will leave you logged on before automatically logging you off. This option reduces the risk of someone signing files with your digital signature or decrypting your files while you are temporarily away from your computer. You can set this number between 1 and 60 minutes. Enter a value that suits your needs.

Note: For information about the other options you can set, refer to "Setting options for Entrust/Client" on page 116.

10. Click *OK* in the *Entrust Options* dialog.

The *Entrust* main window appears. You can begin using Entrust.



You can now encrypt, decrypt, sign, and verify files. You can also create your address book, create recipient lists, change your password and securely delete files.

Note: If you have not already done so, destroy the reference number and authorization code you used to create your Client username.

Recovering your Entrust/Client username

You will need to recover your username if

- you forget your password
- you lose your Client profile
- your Client profile becomes corrupt

Before you can recover your username, you need to contact your Administrator to obtain a new reference number (for example, 91480170) and an authorization code (for example, CMTJ-8VOR-VFNS). If you do not have this information already, contact your Entrust Administrator to obtain it. Your Administrator will tell you your reference number and authorization code in a confidential and secure manner.

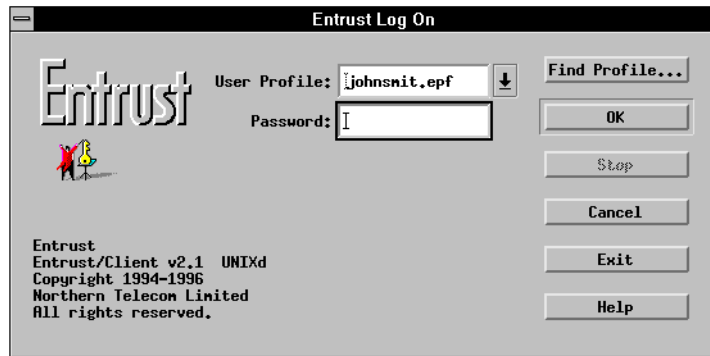
ATTENTION

Keep your reference number and authorization code confidential. Ensure you destroy them after you have recovered your Client username.

Once you have this information, you can recover your username by following these steps:

1. Start up Entrust as you usually do.

The *Entrust Log On* dialog appears.



2. Click *Cancel*.

The *Entrust* main window appears.

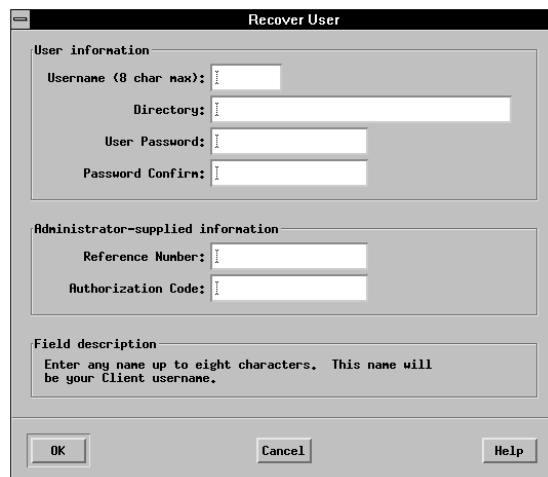
3. Choose *Recover User...* from the *File* menu.

The *Recover Profile* dialog appears.

The 'Recover Profile' dialog box has a title bar with a minus sign. The main area contains two paragraphs of text: 'If you have an existing Entrust profile that you would like to recover then enter the full path name of the profile and click Continue.' and 'If you do not have an existing profile (it has been lost or deleted), then leave the Existing profile field empty and press Continue.' Below the text is a text field labeled 'Existing profile' with a 'Browse...' button to its right. At the bottom are three buttons: 'Continue', 'Cancel', and 'Help'.

4. If you still have a copy of your profile, enter the path to your current profile in the *Existing profile* field. Alternatively, you can click *Browse...* and locate your profile. This case typically applies if you are recovering your Client username because you forgot your Client password. If you no longer have a copy of your profile, continue at step 5.
5. Click *Continue* in the *Recover Profile* dialog.

The *Recover User* dialog appears. Notice the *Field description* area at the bottom of the dialog. This area provides a brief description of the information you need to enter in each field of the dialog. Simply click in any field and the corresponding description will appear in the *Field description* area.

The 'Recover User' dialog box has a title bar with a minus sign. It is divided into three sections. The first section, 'User information', contains four text fields: 'Username (8 char max):', 'Directory:', 'User Password:', and 'Password Confirm:'. The second section, 'Administrator-supplied information', contains two text fields: 'Reference Number:' and 'Authorization Code:'. The third section, 'Field description', contains a text area with the text: 'Enter any name up to eight characters. This name will be your Client username.' At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

6. Enter a name in the *Username* field.

You can choose any name you like, but you are limited to eight characters (for example, *johnsmit*).

Note: If you are reusing an existing profile, the *Username* field is automatically filled in.

7. Tab to the *Directory* field and enter the name of the directory in which you want to store your profile. If the directory does not already exist, the Client will create it.

Note: If you are reusing an existing profile, the *Directory* field is automatically filled in.

8. Tab to the *User Password* field and enter a password.

Your Client password must

- be at least eight characters long (however, as you make your password longer, it becomes significantly more difficult for an attacker to guess the password you select)
- contain at least one upper case letter
- contain at least one lower case letter
- not contain many occurrences of the same character
- not be the same as your Client username
- not contain a lengthy substring of your Client username

The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: \$, +, =, !, ~, ^ and &. A good password is one that is difficult to guess yet easy to remember (for example, H2OPlsNow! (water please, now!)). For more information about passwords, refer to "Appendix C: Entrust password security."

9. Tab to the *Password Confirm* field and enter the same password again.

The reason you need to enter your new password twice is to ensure you typed exactly what you intended to type. The Client checks to ensure that you entered your new password exactly the same way both times.

If you write down your password, store it in a locked place to which only you have access.

10. Tab to the *Reference Number* field and enter the reference number you obtained from your Administrator (for example, 91480170).
11. Tab to the *Authorization Code* field and enter the authorization code you obtained from your Administrator (for example, CMTJ-8VOR-VFNS). The hyphens are optional.

12. Click *OK*.

After a short period of time, the *Entrust Options* dialog appears if Entrust was able to recover your username. The *Entrust Options* dialog contains tabs that let you choose various types of options you want to change.



Note: If Entrust was unable to recover your username, try supplying the information again. Ensure that you enter the reference number and authorization code in exactly the same form as you received them from your Entrust Administrator. If you still cannot create a Client username, contact your Administrator.

- 13.** Notice the *Logoff timeout* field in the *Entrust Options* dialog. This field specifies the length of time during which the Client will leave you logged on before automatically logging you off. This option reduces the risk of someone signing files with your digital signature or decrypting your files while you are temporarily away from your computer. You can set this number between 1 and 60 minutes. Enter a value that suits your needs.

Note: For information about the other options you can set, refer to "Setting options for Entrust/Client" on page 116.

14. Click *OK*.

The *Entrust* main window appears.

Your username has been recovered. You can resume use of the Client.

Note: If you have not already done so, destroy the reference number and authorization code you used to recover your Client username.

Setting options for Entrust/Client

You can change values of some Client options from the *Entrust Options* dialog. These values remain in effect until you change them again.

To access the *Entrust Options* dialog, choose *Options...* from the *File* menu. Alternatively, you can click *More Options...* in the *Encrypt and Sign* dialog.

The *Entrust Options* dialog contains tabs that let you choose various types of options you want to change.



The *Entrust Options* dialog contains the following types of options:

- general option
- encrypt and sign options

General option

Logoff timeout

The Client automatically logs you out a preset number of minutes after you last used the Client. You can choose to set this number to between 1 and 60 minutes. Enter a value that suits your needs. This option reduces the risk of someone signing files with your digital signature or decrypting your files while you are temporarily away from your computer.

Encrypt and sign options

Click the *Encrypt/Sign* tab in the *Entrust Options* dialog to access the encrypt and sign options.



Compress before encrypting

Select this option to compress the files before they are protected. It is necessary to compress files before they are encrypted because it is impossible to compress an encrypted file. By definition, an encrypted file is completely random, making compression impossible. The amount of compression depends on the type of file. Word processing files can generally be compressed to less than half their original size. Graphics files can often be compressed even more than word processing files.

ASCII encode after encrypting

Select this option to force the Client to use an ASCII file format when encrypting files. If you do not select this option, the Client will use a binary format. The advantage of using the binary format is that the resulting size of the protected file will be about 30% smaller than if you use the ASCII file format, and it will take a shorter time to process files. However, the ASCII option is mandatory if you plan to transfer the protected file using an electronic file transfer mechanism like ASCII-FTP or certain electronic mail systems that can only handle ASCII file formats.

Output file extension

Once your file is protected, its filename will receive the suffix specified in the *Output file extension* field. The default suffix is *ent*. You can change the output file suffix by entering a different one. It is recommended that you use the default *ent* suffix to achieve consistency among Client users across all supported platforms. Using the default also makes it easier to find protected files. For example, if you protect a file called *report7.doc*, the filename of the protected file is *report7.doc.ent*.

Encryption Method

CAST and DES are two encryption methods available to the Client to protect your files. Typically, the decision on which to use is a policy adopted by your organization with guidance from your Administrator.

Using Entrust/Client on different computers

You can use the Client on any computer in your organization that has the Client installed (for example, Macintosh computers, UNIX workstations, and PCs running Microsoft Windows). All you need to do is make a copy of your Client profile (for example, *johnsmit.epf*) and transfer it to the computer you want to use by means of a floppy diskette or some electronic file transfer mechanism. You should also transfer a copy of your recipient lists file (for example, *johnsmit.erl*) to the same directory as your profile. If you intend to use your address book to protect files for users outside your CA security domain, you must also transfer the file containing your address book (for example *johnsmit.pab*) to the same directory as your profile.

ATTENTION

Even though your personal information stored in your profile is encrypted, you should still take precautions to ensure nobody obtains a copy of your profile. You need to be particularly careful when transferring your profile across various computers.

You may need to rename your profile when you move it among different platforms. The profile name must conform to the filename conventions used by the new platform. For example, if you move your profile from a Macintosh to a UNIX platform, you will need to rename your profile from *John Smith* to *johnsmit.epf*. When you transfer your recipient list file (*.erl*) and personal address book file (*.pab*), do not change the filename extensions.

When you start the Client on the new platform, use the *Find Profile...* button on the *Entrust Log On* dialog to locate your Client profile on that computer and select your profile.

ATTENTION

For increased security, your Entrust information, which is stored in your profile, is automatically updated from time to time. Therefore, you should only keep one copy of your profile. When you need to use a different computer, transfer your profile and delete it from the previous computer. This way, your profile will always contain the most current Entrust information. Transfer the updated copy of your address book file to your other computers if you make changes to your address book. Similarly, transfer an updated copy of your recipient lists file (*erl* filename suffix) if you make changes to any recipient list information.

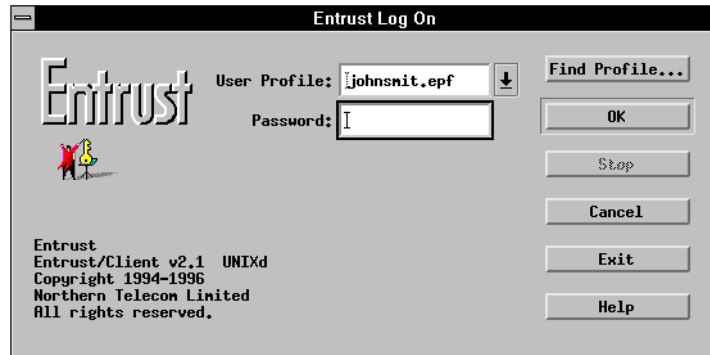
Starting Entrust/Client

This procedure assumes that you have added the directory containing the Client software to your path. If you have not, you will need to enter the absolute path to the *xentrust* executable.

To start the Client, enter

```
% xentrust
```

The *Entrust Log On* dialog appears. You can now log on to the Client. Refer to “Logging on to Entrust/Client” on page 121 for more information.



If the *Welcome to Entrust* dialog appears instead of the *Entrust Log On* dialog, you probably have not yet created your Client username. Click *Create User...* and skip to step 2. in “Creating additional Entrust/Client usernames” on page 108.



Logging on to Entrust/Client

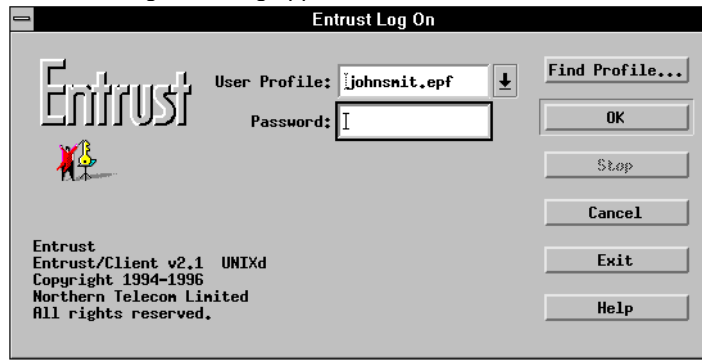
Logging on to the Client is different from starting the Client. Starting the Client involves invoking the application. You cannot use the Client until you log on as an Entrust user. The purpose of logging on is to authenticate yourself to the Client through the use of a password.

Since Entrust has a safety feature that logs you off a preset number of minutes after you last used the Client, it is possible that you were automatically logged off. You can set the number of minutes to timeout in the *Entrust Options* dialog. To access the *Entrust Options* dialog, choose *Options...* from the *File* menu. If you attempt to use the Client while you are logged off, you will automatically be prompted to log on.

To log on to the Client, proceed as follows:

1. Select any Client function and you will be prompted to log on to Entrust if you are not already logged on.

Alternatively, you can choose *Log on as Entrust user...* from the *File* menu. The *Entrust Log On* dialog appears.



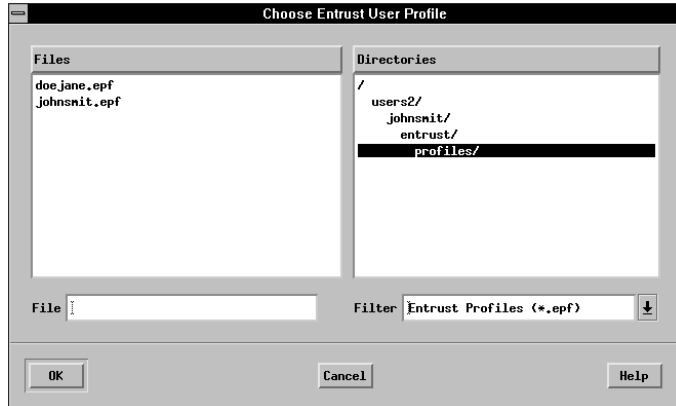
2. Verify that your profile name appears in the *Entrust Log On* dialog (for example, *johnsmit.epf*).

If your profile name does appear, skip to step 3.

If your profile name does not appear, proceed as follows:

- a. Click *Find Profile...* in the *Entrust Log On* dialog.

The *Choose Entrust User Profile* dialog appears.



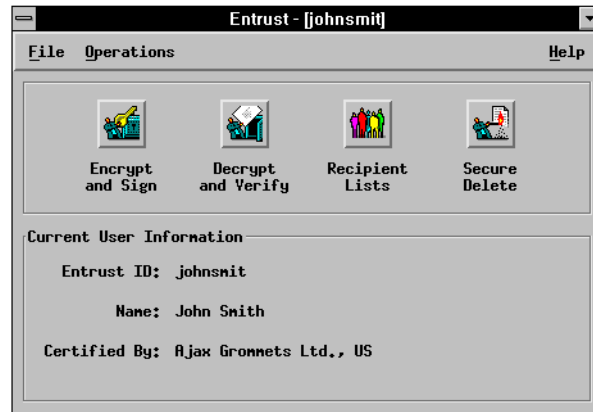
- b. From the *Choose Entrust User Profile* dialog, locate your Client profile (for example, *johnsmit.epf*). If necessary, change directory.
- c. Select your profile once you have found it.
- d. Click *OK* in the *Choose Entrust User Profile* dialog.

The *Entrust Log On* dialog reappears displaying the name of your profile.

If you cannot locate your profile, contact your Entrust Administrator.

3. Enter your password in the *Entrust Log On* dialog. Remember that your password is case-sensitive.
4. Click *OK*.

The *Entrust* main window appears.



You can now begin using the Client.

Logging off from Entrust/Client

To protect yourself and your information, you can log off from the Client to prevent an intruder from decrypting your protected files, signing files on your behalf, or securely deleting your files while you are away from your computer.

Logging off does not close the Client; it simply prevents anyone from using your Client username without your authorization.

There is also a log off time-out that automatically logs you off if you do not use the Client for a period of time. You can set the number of minutes for the automatic log-off time-out in the *Entrust Options* dialog. To access the *Entrust Options* dialog, choose *Options...* from the *File* menu.

To log off from the Client, choose *Log Off...* from the *File* menu.

Ending your Entrust/Client session

To end your Client session, choose *Exit* from the *File* menu.

Hints

Forgotten password or lost or damaged Client profile

If you forget your Client password, or if your Client profile becomes lost or damaged and you do not have a backup, you must recover your Client profile. Ask your Entrust Administrator for help.

Using Entrust/Client in different time zones

If you ever change the current time on your computer (for example, because you brought your laptop computer with you to a different location) you should also change the time zone setting that corresponds to your new location. The time on the computer you use to run Entrust/Client must be within two hours of the current time on the clock on which its corresponding Entrust/Manager is running. (Entrust/Manager is the Entrust component that manages all Entrust addresses within your CA security domain.) If your time zone setting does not correspond to your current location, the time zone setting may be sufficiently different to cause a difference in time greater than two hours. To change the time zone, edit the *TZ* environment variable. Examples of North American time zones are as follows:

- EST5EDT (Eastern Standard Time)
- CST6CDT (Central Standard Time)
- MST7MDT (Mountain Standard Time)
- PST8PDT (Pacific Standard Time)

If the time zone setting or the time is incorrectly set on your computer, you may receive a message similar to one of the following when you try to log on to the Client:

`Could not retrieve up to date certificate revocation list.`

or

The Entrust/Manager time and the time on this machine differ significantly. Please set the time on your machine correctly and then try again. Contact your Entrust Administrator if you continue to experience difficulty.

If you do not change the time on your computer when you move across time zones, you do not need to change the time zone setting.

Intended recipient cannot decrypt my files

Problem

A recipient cannot decrypt a protected file that came from you.

Solution

First, try to decrypt the file yourself as a test. If you are able to decrypt the file, it is possible the protected file was damaged in transit. Give the recipient a new copy of the protected file.

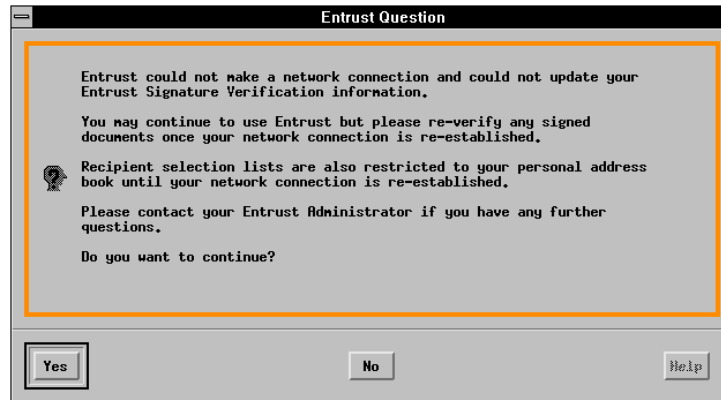
If the person still cannot decrypt the file, check the mechanism you used to give the recipient the protected file. If the file transfer mechanism requires ASCII formatted files, ensure that you used the *ASCII encode after encrypting* option when you protected the file.

If the recipient is in a CA security domain that is different from yours, ask the person to give you a new *key* file and import it again into your address book. Then protect the original file again and give a new copy to your recipient.

If the recipient still cannot decrypt the file, contact your Administrator.

Cannot update your Entrust signature verification information

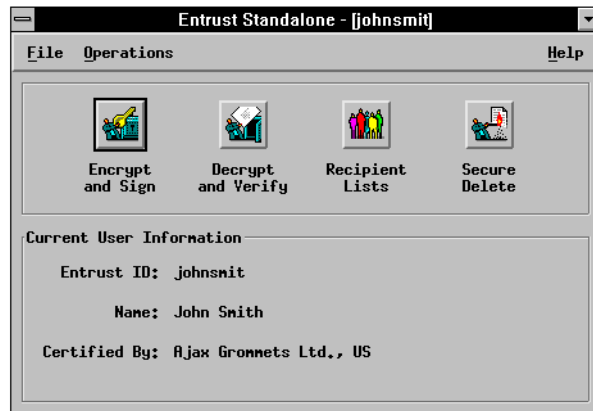
If the following dialog appears when you log on to Entrust/Client, it is likely that you do not have a network connection. There are many possible causes for loss of network connection. The most common cause is that a server is not functioning properly.



If you choose to continue, you will still be able to use the Client to decrypt files. You will also be able to encrypt files for people listed in your address book and for people who are members of recipient lists to which you still have access. However, you will not be able to create new usernames, recover a username or encrypt files for people who are not listed in your address book or recipient lists.

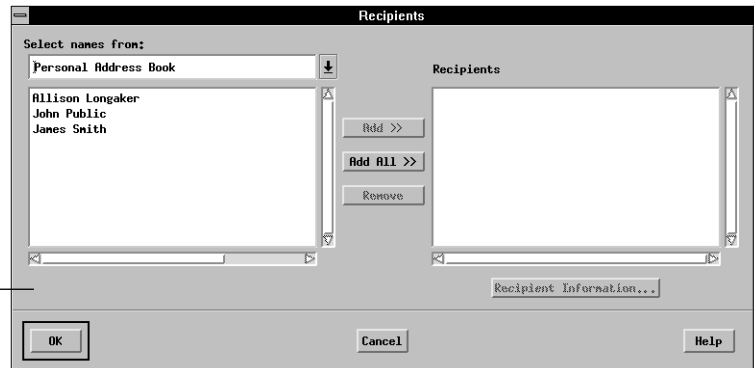
Although the Client will allow you to verify signatures when there is no network connection, you should not necessarily trust the authenticity of the signatures. The reason you should not trust the authenticity of the signatures is that the Client cannot update your Entrust signature verification information. Without access to this information, the Client cannot verify the validity of the signature that was used to sign the file. Once your network connection has been established again, ensure you reverify every signature that you verified while the Client was not connected to the network.

Once you are logged to the Client, you will notice the word *Standalone* in the window title bar of the *Entrust* main window. This will remind you that you are running the Client without a network connection.



Search information is unavailable

The search field(s) normally appear in this area.



Problem

The search information field(s) are unavailable in the *Recipients* dialog.

In this situation you will only be able to encrypt files for people listed in your address book and for people who are members of recipient lists to which you still have access.

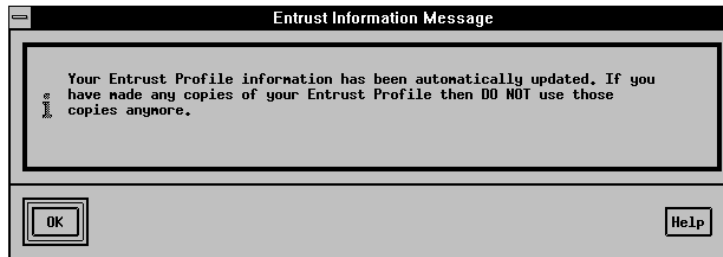
Reason

The probable reason is that you do not have a network connection. For more information about this situation, refer to “Cannot update your Entrust signature verification information” on page 127.

Logging on to the Client after your personal Entrust information has been changed

Problem

The following message appears after you log on to the Client.

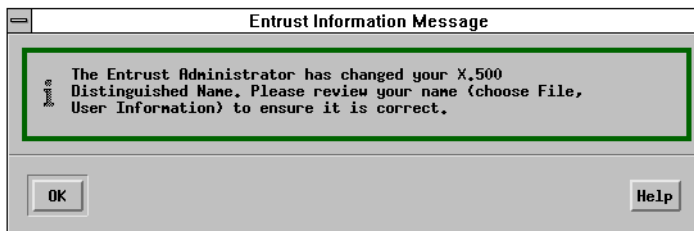
**Reason**

This message appears because some of your personal Entrust information has been automatically updated. This information is stored in your Client profile. Therefore, if you already made copies of your profile, as described in “Using Entrust/Client on different computers” on page 119, you should replace those outdated copies as soon as possible.

Logging on to the Client after your name has been changed

Problem

The following message appears when you attempt to log on to the Client.



Reason

This message appears because the Entrust Administrator has changed your name in the Entrust database. Typically this is because you legally changed your name within the corporate database and the change is being reflected within Entrust.

Another reason the message appears might be that, for some reason, your name and your Entrust information has been moved to a different location in the corporate database. Typically a change such as this affects many people at the same time and you will find that other users are also getting the same message when they log on to the Client. If you have not changed your name, ask your Entrust Administrator for an explanation.

Importing a key certified by a CA with the same name as your CA

Problem

The following message appears when you attempt to import a *key* file into your address book.

**Reason**

This message appears because the address in the *key* file you attempted to import into your address book was certified by a Certification Authority that is different from yours but has the same CA name. This provides a safeguard to prevent people in other CA security domains from masquerading as users certified by your CA.

Appendix A: Entrust/Client shortcuts

You can use the mouse to perform all Client functions. Alternatively, you can use the keyboard. This appendix describes the keys you need to navigate through Entrust.

Hot keys

You can use *hot* keys to navigate. *Hot* keys are used by pressing and releasing the *F10* function key and then pressing two keys in succession. For example, Figure 3 shows the result of pressing and releasing the *F10* function key followed by the *f* key while the *Entrust* main window is displayed. Notice the underlined letters in the menu. The underlined letters indicate which keys are *hot*.

Figure 3 Result of pressing the F10 function key followed by the f key

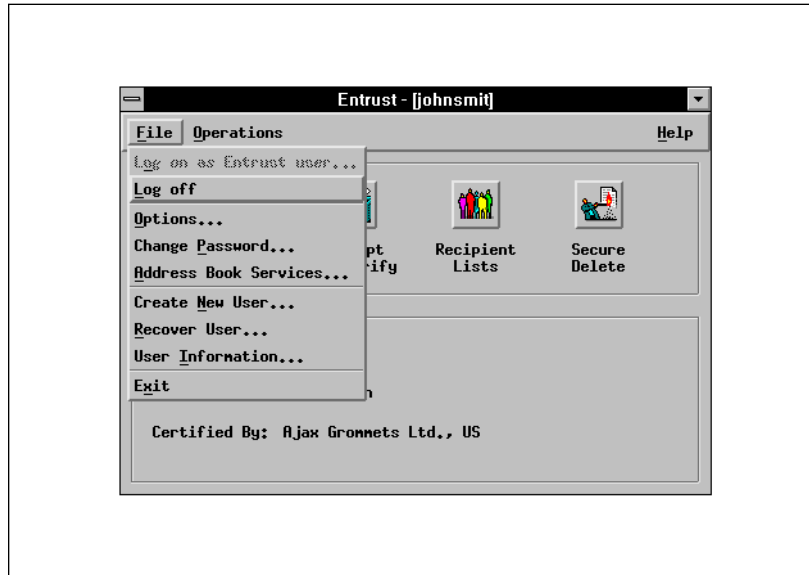
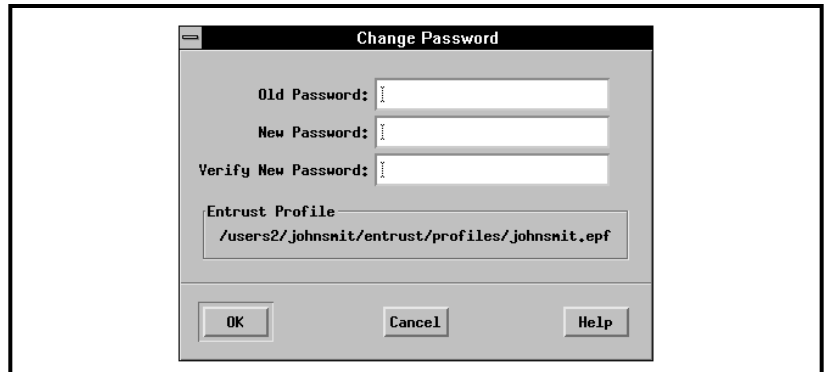


Figure 4 shows the dialog that appears after you press and release the *p* key after having pressed and released the *F10* function and *f* keys.

Figure 4 Result of pressing the F10 function key followed by the *f* and *p* keys



From any Client menu you can press and release the *F10* function key followed by pressing an underlined key to access the function you want to perform.

You can also use the directional keys in conjunction with *hot* keys. After you display a pull-down list, use the directional keys to highlight the function you want.

Tab key

Press and release the *Tab* key to move from item to item in a dialog. Each press and release combination highlights the next item. An item can be anything in the dialog (for example, buttons, fields, or scrollable lists). Press the *Tab* key until the item you want is highlighted.

Shift key

Use the *Shift* key in conjunction with the *Tab* key to reverse the order in which items are highlighted. For example, if you press the *Tab* key one too many times and miss the item you want, you can hold down the *Shift* key and press the *Tab* key to move to the correct field.

Enter key

Pressing the *Enter* key causes Entrust to perform the function assigned to that key. When you first display a dialog, there is always a default button that is already highlighted. You can change which key is highlighted by pressing the *Tab* key.

Appendix B: Entrust/Client user files

Client_username.epf

This file contains your Client profile. This profile contains your personal information which is required by the Client. This critical information is encrypted to ensure security. For increased security, you can store this file in a directory to which only you have access.

By default, the filename for the profile is your Client username followed by the *epf* filename extension (for example, *johnsmit.epf*).

This file is platform-independent, which means you can transfer this file to any computer in your organization running the Client and use it to log on to the Client. You may, however, need to rename your profile when you transfer it to another computer. For more information, refer to “Using Entrust/Client on different computers” on page 119.

ATTENTION

Do not delete or alter this file in any way. If you do, you will need to ask your Administrator to help you recover your profile.

Client_username.erl

This file contains all your recipient lists, including any links to shared recipient lists you may have imported. By default, the filename is the same as your username. An *erl* filename extension (for example, *johnsmit.erl*) is automatically added to the filename of the recipient lists file.

An Entrust/Client recipient list is a set of encryption and signing options, and a set of recipients that you select and store under a *recipient list* name. Instead of having to specify each recipient and option every time you want to encrypt a file, you can specify the name of a recipient list.

Refer to “Using saved lists of recipients” on page 93 for more information.

filename.srl

This file contains a single recipient list that has been designated as a shared recipient list. It is created by exporting a single recipient list. You can choose any filename when you export this file but the filename automatically receives an *srl* filename extension (for example, *ourgroupp.srl*). Refer to “Sharing recipient lists” on page 101 for more information.

Client_username.key

This file contains your personal Client address. By default, the filename comprises your Client username with a *key* filename extension (for example, *johnsmit.key*).

If you want a person who uses the Client outside your CA security domain to encrypt a file for you or to verify a file signed by you, give that person a copy of this file. When that external Client user encrypts a file for you, this file will provide the necessary information that will ensure you will be able to decrypt the file. See “Exchanging protected files with users in different domains” on page 83.

Client_username.pab

This file contains your address book. By default, the filename comprises your Client username with a *pab* filename extension (for example, *johnsmit.pab*).

The address book contains addresses of people who use the Client outside your CA security domain. These addresses allow you to encrypt files for these people so that they will be able to decrypt them.

For more information, refer to “Exchanging protected files with users in different domains” on page 83.

entrust.ini

This file contains important information required by the Client software. It is important not to modify the contents of this file or to delete the file. It is normally stored in your home directory and should not be moved.

.entrustrc

This file contains the following lines:

ENTRUSTDIR=*parent_directory/entrust*

XNLSPATH=

LASTPROFILE=

See Figure 5 for a sample *.entrustrc* file.

The text to the right of ENTRUSTDIR= should be the directory in which the Client was installed (for example, */opt/entrust*). This text is automatically inserted by the *setup* script.

The text to the right of XNLSPATH= should be blank on all platforms except SunOS 4.1.3 in which case it should be *parent_directory/entrust/lib/nls*, where *parent_directory* refers to the directory in which the Client is installed.

The text to the right of LASTPROFILE= should be the path to your Client profile unless you have not yet used the Client in which case it should be blank. When you start up the Client, it checks for the *.entrustrc* file in your home directory. If it finds it, it displays the Client username that it finds to the right of LASTPROFILE variable. Leaving this field blank is harmless.

A copy of the *.entrustrc* file should be stored in each user's home directory.

Figure 5 Sample .entrustrc file

```
ENTRUSTDIR=/opt/entrust
XNLSPATH=/opt/entrust/lib/nls
LASTPROFILE=/users/johnsmit/johnsmit.epf
```

Appendix C: Entrust password security

Password security is a major concern for computer users. Exhaustive password-searching attacks and dictionary attacks (two common methods for cracking passwords) represent serious threats to computer security. When you consider that an HP700 UNIX workstation can perform an exhaustive search of all possible combinations of six-letter (lower case) UNIX passwords in only 17 hours, it appears relatively easy for intruders to break into your system.

We understand your concerns. Passwords represent a critical link in the security chain. As a result, Entrust takes important steps to protect all passwords from even the most highly sophisticated schemes for attacking passwords.

When a user chooses a password, Entrust enforces the following rules to ensure that the password is secure:

- The password must contain a minimum of eight characters.
- The password must contain at least one upper case letter.
- The password must contain at least one lower case letter.
- The password must not contain many occurrences of the same character.

The maximum number of occurrences of the same character allowed in your password is half the length of your password. For example, *mGmdmm&m* is not valid even though it contains eight characters. It is not valid because it contains five occurrences of the character *m* which is more than half the length of the password. The password *mGmtdm&m* is valid because it contains eight characters and it only contains four occurrences of the character *m* which is exactly half the length of the password.

- The password must not be the same as your Client username.

- The password must not contain a lengthy substring of your Client username.

The maximum length of an allowable username substring is equal to half the length of your password. For example, if a username is *johnsmit*, the password *johnsM*4* is not valid even though it contains eight characters. It is not valid because it contains a five-character substring which can be found in the username, and five is more than half the length of the password. The password *johcmM*4* is valid because it contains eight characters and because it contains only a three-character substring which is less than half the length of the password.

Simply increasing the length of a password makes it less susceptible to attack. For example, increasing the password length from six to eight letters (lower case) changes the time to do an exhaustive search on UNIX passwords from 17 hours to 16 months. Moreover, when digits are introduced into eight-character passwords, the time required to do an exhaustive search on UNIX passwords increases to almost 18 years!

Once a user selects a password, Entrust applies a hash function to the password. Hash functions are often referred to as one-way hash functions, meaning that it is extremely difficult to determine the input to the one-way function if you have only the result of applying the function (that is, the function cannot be reversed). The result of the initial application of the hash function is then run through the hash function again, then again and again—in fact, the hash function is applied 100 times in succession.

Furthermore, prior to hashing, a unique quantity called a salt is appended to each user's password in a unique way. Using a unique salt for each password slows down password searches by attackers. With unique salts, an attacker must perform separate calculations for each password that is attacked. If the salts were not unique, an attacker could create a database of hashed passwords once (assuming the attacker knows the hash function), and then use this database to discover each password.

In addition, the complex calculations required to check a Client password take 50 times longer than the calculations required to check a UNIX password. That means that an attacker using an exhaustive search strategy would take approximately 65 years to search eight-letter (lower case) Client passwords versus only 16 months for equivalent UNIX passwords.

Entrust takes the result of iterating the original password through the hash function 100 times and uses that result as a key to encrypt a known value. The result of the encryption is referred to as the “password check value.” Only the password check value is stored in the user's Client profile. The original password is never stored by Entrust, making it impossible for someone to discover your password using a low-level disk utility program.

Later, when the user enters the original password while logging on to Entrust, the application reapplies the calculations listed above. The resulting check value is then compared against the stored password check value. If the two check values match, the user is allowed to log on to Entrust. Otherwise, the attempted log-on is rejected.

A more sophisticated attack than trying all combinations of characters is to guess dictionary words as passwords (known as a dictionary attack). While Entrust takes important steps to thwart dictionary attacks, users can further protect their passwords by taking the following precautions:

- using a mixture of letters (upper and lower case), digits, and special characters (for example, @ and !)
- creating passwords longer than eight characters
- avoiding words found in dictionaries

Note: Calculations used in this appendix are done assuming computing capabilities equivalent to those in an HP700 UNIX workstation.

Appendix D: Entrust specifications

Cryptographic algorithms and standards

Encryption

- U.S. Data Encryption Standard (DES) in accordance with U.S. FIPS PUB 46-2 and ANSI X3.92
- Northern Telecom CAST algorithm
- DES and CAST encryption using CBC mode of operation in accordance with U.S. FIPS PUB 81, ANSI X3.106 and ISO/IEC 10116

Digital signatures

- RSA digital signature in accordance with RSA Data Security Inc. Public Key Cryptographic Standards (PKCS) specification PKCS#1

Hash functions

- MD2 Message-Digest algorithm in accordance with Internet RFC 1319
- MD5 Message-Digest algorithm in accordance with Internet RFC 1321

Key management

- RSA key transfer in accordance with Internet RFC 1421 and 1423 (PEM)

Integrity

- Message Authentication Code (MAC) in accordance with U.S. FIPS PUB 113 and ANSI X9.9

Pseudo-random number generation

- As given in ANSI X9.17

Data formats and protocols

Certificate formats

- Public-key certificates in accordance with ITU-T Rec. X.509 (1993), ISO/IEC 9594-8 (1995), and Draft Amendment 1 to ISO/IEC 9594-8 (1995)
- Certificate revocation lists in accordance with ITU-T Rec. X.509 (1993), ISO/IEC 9594-8 (1995), and Draft Amendment 1 to ISO/IEC 9594-8 (1995)
- RSA algorithm identifiers and public key formats in accordance with Internet RFC 1422 and 1423 (PEM)

File envelope format

- Based on Internet RFC 1421 (PEM)

Directory protocols

- Directory Access Protocol (DAP) and Directory System Protocol (DSP) in accordance with ITU-T Rec. X.500 and ISO/IEC 9594
- Lightweight Directory Access Protocol (LDAP) in accordance with Internet RFC 1777
- Entrust/Server is based on the University of Michigan's LDAP server, ldapd

Client management protocol

- Northern Telecom Security Exchange Protocol (SEP), built using Generic Upper Layers Security (GULS) standards based on ITU-T Recs. 830, 831, 832 and ISO/IEC 11586-1, 11586-2, 11586-3

Software interfaces

Application program interfaces (APIs)

- Online mode API in accordance with Internet Generic Security Services (GSS)-API specification in Internet RFCs 1508 and 1509
- Online mode GSS-API mechanism using Internet Simple Public Key Mechanism (SPKM) (proposed Internet Standard)
- Store-and-forward API in accordance with Entrust/Toolkit API specification

Government endorsement

- Cryptographic module validation to level 1 under U.S. FIPS PUB 140-1
- Canadian Government Cryptographic Endorsement and Assessment Program (CEAP) (evaluation in progress)

List of terms

address book

An address book contains the Entrust addresses of people in other organizations with whom you plan to exchange protected files.

Administrator

See Entrust Administrator.

authorization code

A code (for example, CMTJ-8VOR-VFNS), obtained from your Entrust Administrator, which is required along with a reference number to create a new Entrust/Client username or to recover an existing username. The authorization code can only be used once and then it is no longer valid.

CA

See Certification Authority.

CA security domain

A CA security domain is a group of Entrust users who have all been certified by the same Certification Authority (CA) under one software license.

Typically these users have something in common (for example, they all work in the same company or they work on the same project). It is possible to have several Entrust domains in the same company. What differentiates one domain from another is the CA that certifies the domain.

Certification Authority (CA)

Typically, in each organization there are people who are responsible for setting policies regarding the protection of sensitive and valuable data. Within the context of Entrust, these people are referred to collectively as the Certification Authority (CA). The people who are responsible for implementing these security policies are called Security Officers and Entrust Administrators. These people act on behalf of the CA.

Client

See Entrust/Client.

decrypt

To decrypt a protected file is to restore it to its original, unprotected state.

defaults

Various operations, options, and entry fields have default values in Entrust/Client. These values can be changed in the *Entrust Options* dialog.

destination directory

In the Client, the designated directory that receives protected or decrypted files.

digital signature

The result of making a mathematical summary (known as a *hash*) of data and signing the hash with a signing private key known only to a specific authorized user. The signature can be verified by any other user who has the corresponding verification public key. A digital signature provides a guarantee to a recipient that a file came from the person who sent it, and that it was not altered since it was signed.

domain

See CA security domain.

encrypt

To encrypt a file is to render the file completely unreadable. That means no one, including you, can read the file until it is decrypted. Only you and the authorized recipients can decrypt the file. You have full control in determining authorized recipients.

Entrust address

An Entrust address provides the necessary information to ensure that files encrypted and signed by someone using Entrust in one organization can be decrypted and verified by someone using Entrust in other organizations.

An Entrust address is stored in a *key* file and all users can export their own *key* file. The filename comprises your Client username with a *key* filename extension (for example, *johnsmit.key*). For information about exporting your Entrust address, refer to “Exporting your personal Entrust address” on page 91.

Entrust domain

See CA security domain.

Entrust Administrator

This is a person within your organization who has the responsibility of maintaining all aspects of the Client. This job includes enabling and recovering Client users. The Administrator should be trusted by everyone in the CA security domain.

Entrust/Client

A software application that allows people to encrypt files, decrypt files, digitally sign files, and verify digital signatures on files.

Entrust/Manager

A database that manages cryptographic keys for Entrust users.

Entrust/Client profile

A file containing critical information about you which is required by the Client. This critical information is encrypted to ensure security.

For increased security, you can store this file in a directory to which only you have access.

Regardless of where you store your profile, you must ensure that no one can get access to it.

Entrust recipients

People whom you have authorized to decrypt some of your files.

hot keys

Key patterns used to navigate through Entrust as an alternative to using the mouse. Usually these involve pressing and releasing the *F10* function key and then pressing two keys in succession that relate to underlined letters in a menu.

personal address book

See address book.

profile

See Entrust/Client profile.

recipient

See Entrust recipients.

recipient list

An Entrust/Client recipient list is a set of encryption and/or signing options, and/or a set of recipients that you select and store under a *recipient list* name. Instead of having to specify each recipient and/or option every time you want to encrypt a file, you can specify the name of a recipient list.

Refer to “Using saved lists of recipients” on page 93 for more information.

reference number

A number (for example, 91480165), obtained from your Entrust Administrator, which is used along with an authorization code to create a new Entrust/Client username or to recover lost data associated with an existing user.

secret

In this document, secret refers to information that should not be divulged to anyone. For example, passwords must remain secret.

validation string

A validation string is a string of alphanumeric characters (for example, 7CN4-YL5D-HP7V) that is automatically generated by the Client when you export your address. Each Entrust address has a unique validation string which is associated with the *key* file. Use the validation string to confirm that the address someone gives you in a *key* file has not been modified since it was created.

X Windows

X Windows: Copyright 1991 by the Massachusetts Institute of Technology (MIT). Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of MIT not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. MIT makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

Index

A

- address book 6, 57, 84
 - accessing your 84
 - adding names to 86
 - building your personal 86
 - changing contents of 89
 - changing names in 89, 90
 - creating 84
 - deleting people from 89
 - file 134
 - importing addresses into 86
 - re-importing names into 90
 - removing people from 89
- address, exporting your 91
- Administrator 2, 147
- APIs. *See* application program interfaces
- application program interfaces 143
- Archive option 7, 39, 68
- ASCII encode output file(s) option 9, 118
- ASCII file format 7, 9, 69, 118
- authentication 5, 6
- authorization code 16, 28, 109, 114, 145
- automatic log off 29, 31, 47, 110, 115, 116

B

- binary format files 9, 69

C

- CA security domain 145
- CA. *See* Certification Authority
- CAST 118
- Certification Authority 2, 45
- changing
 - recipient lists 94, 98
 - your password 106
- Client 2
 - ending your session 45, 124
 - installing 19
 - logging off 124
 - logging on 121
 - password. *See* password
 - profile. *See* profiles
 - starting 120
 - starting for the first time 26
 - user files 133
 - using in different time zones 125
 - using on different computers 119
 - using with e-mail 11
 - See also* Entrust
- Client username, recovering 112
- Compress before encrypting option 69, 117
- compression 7

- creating
 - a new user 26, 108
 - additional usernames 108
 - recipient lists 94, 95
 - your address book 84
- cryptographic algorithms 141
- D**
- data
 - integrity 5
 - privacy 5
- data formats 142
- decrypting and verifying icons 82
- decrypting, files 76, 81
- deleting
 - files securely 73
 - people from your address book 89
 - recipient lists 94, 100
- DES 118
- destination directory. *See* directories
- digital signature. *See* signatures
- directories
 - encrypting 48
 - for decrypted files 43
 - for encrypted files 39
 - protecting 48
 - signing 48
- domain 2, 83, 145
- duplicating an existing recipient list 95
- E**
- editing
 - recipient lists 94, 98
 - your address book 89
- electronic
 - file transfer 13
 - mail 13
- e-mail use with Client 11
- Encrypt and Sign dialog, accessing 48

- encrypted files 8
- encrypting
 - files and directories 48
 - operations 66, 95
 - options 117
- encrypting and signing process 70
- encryption
 - definition 8
 - example 11
 - methods, CAST and DES 118
 - selecting files for 48
- ending your Client session 45, 124
- endorsement 143
- ent file 41, 69, 72, 118
- Enter key 132
- Entrust
 - across different platforms 119
 - address 83, 91, 146
 - Administrator 2, 147
 - domain 83
 - information update 129
 - main window 30
 - profiles. *See* profiles
 - recipients 147
 - using on different computers 119
 - See also* Client
- entrust.ini file 21
- Entrust/Client. *See* Client
- entrustrc file 134
- epf file 27, 133
- erl file 93, 133
- example
 - of encrypting 11
 - uses of Client 10
- exporting your personal address 91

- F**
- filename
 - for Entrust address 83, 146

filename (*continued*)

- of encrypted file 69, 118
- with ent suffix 69, 118
- with epf extension 27, 133
- with erl extension 93, 133
- with key extension 83, 134, 146
- with pab extension 84, 134
- with srl extension 134

files

- .entrustc 134
- address book 134
- archiving 7
- ASCII format 7, 9, 69, 118
- binary format 9, 69
- compression 7
- decrypting 76, 81
- deleting securely 73
- encrypting 48
- entrust.ini 21, 134
- epf 133
- exchanging between domains 83
- increase in size of 41, 72
- key 83, 84, 87, 91, 92, 146
- pab 84, 134
- personal address 134
- profile 27, 133
- protected 76
- protecting 8, 48
- recipient list 133
- secure deletion 7
- shared recipient list 134
- signing 48
- tampered 10, 82
- transferring 13
- verifying 76, 81

G

- general option 116
- groups. *See* recipient lists

H

- hash functions 141
- help 18
- hint 125
- hot keys 131

I

- icons, decrypting and verifying 82
- importing
 - addresses 86
 - recipient lists 94
- ini file 134
- installing Entrust/Client 19
- integrity 6

K

- key file 83, 84, 87, 91, 92, 134, 146
- key management 5
- keyboard shortcuts 131

L

- log
 - off 124
 - off automatically 29, 31, 47, 110, 115, 116
 - on 121
- Logging 124

M

- main window 30
- minimum system requirements 15
- multiple search bases 7, 34

N

- name change 130
- no network connection 127

O

- operations

operations (*continued*)

- Encrypt 66, 95
- Encrypt & Sign 66, 95
- Sign 66, 96
- options 28, 31, 38, 47, 116
 - Archive 39, 68
 - ASCII encode after encrypting 69
 - ASCII encode output file(s) 118
 - automatic log off 116
 - Compress before encrypting 69, 117
 - encrypting 117
 - encryption methods 70, 97
 - general 116
 - Output file extension 69, 118
- options, changing default settings 70, 116
- Output field 67, 78

P

- pab file 84, 134
- password 17
 - changing your Client 106
 - forgotten 125
 - guidelines 17, 28
 - rules 17, 27
 - security 17
 - security features of 137
- portability 6
- privacy 5, 6
- profiles 27, 133
 - finding 26, 120
 - selecting 26, 120
- protecting files and directories 48
- protocols 142

Q

- quitting the Client. *See* ending your Client session

R

- recipient lists 39, 93
 - changing 98
 - creating 95
 - creating new 94
 - deleting 94, 100
 - duplicating 95
 - editing 94, 98
 - filename extension 133
 - functions for managing 93
 - importing 94
 - saving 39
 - shared 6
 - sharing 94, 101
- recipients 13, 147
 - creating new recipient lists 94
 - list of 6
 - selecting 51
 - selecting by name 52
 - selecting by recipient list 61, 63
 - selecting from address book 57
- recovering your Client username 112
- reference number 16, 28, 109, 114, 148
- removing people from your address book 89

S

- sample uses of Client 10
- search bases 7, 34
- search fields 34
- search fields unavailable 128
- Secure Delete function 73
- secure file deletion 7
- selecting
 - default encrypt operations 117
 - files for decryption and/or verification 43
 - files for encryption and/or signing 48
 - recipients 33

selecting (*continued*)
 recipients by name 52
 recipients by recipient list 61, 63
 recipients from address book 57
sending protected information 9, 10, 11, 12, 91
shared recipient list file 134
shared recipient lists 94, 101
 filename extension 134
shift key 132
shortcuts 131
signatures
 authenticating 5
 definition 10
 verifying 76
signing
 documents 10
 example of 12
 files and directories 48
 selecting files for 48
srl file 134
standards 141
starting
 Client 120
 Client for the first time 26
start-up package 16

system requirements 15

T

Tab key 132
tampered files 10, 82
terminology 2
transferring protected files 13
troubleshooting. *See* hints

U

unavailable search fields 128
update of Entrust information 129
user 2
usernames 27
 creating additional 108
users external to your domain 83
using the Client in different time zones 125

V

validation strings 83, 87
verifying
 files 76, 81
 signatures 76

Nortel Secure Networks

Entrust/Client

User Guide

for UNIX

© 1994–1996 Northern Telecom Limited
All rights reserved.

This information is subject to change as Northern Telecom Limited reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

Nortel, Entrust, Entrust/Client, Entrust/Manager are trademarks of Northern Telecom Limited. IBM is a trademark of International Business Machines. Microsoft, Windows, Windows 95, and Windows NT are trademarks of Microsoft Corporation. UNIX is a trademark of X/Open Company Ltd. Macintosh is a trademark of Apple Computer, Inc. RSA is under license from Public Key Partners, Inc. HP is a trademark of Hewlett-Packard Company. SunOS and Solaris are trademarks of Sun Microsystems Inc.

Publication number: 68009.08

Date: August 1996

Software release: 2

Printed in Canada

NORTEL
NORTHERN TELECOM